Integrasi HAIS-Q dan ISA Model dalam Peningkatan Kesadaran Keamanan Informasi untuk Mitigasi Risiko Siber

Danar Retno Sari[1*], Hendra Sanjaya Kusno[2], Nurwahidah Jamal[3], Ezra Hartato Pongtuluran[4], Wahyu Anhar[5]
[1,2,3,4,5]Politeknik Negeri Balikpapan; Balikpapan
e-mail: [1]***danar.retno@poltekba.ac.id,** [2]hendra.sanjaya@poltekba.ac.id,
[3]nurwahidah.jamal@poltekba.ac.id, [4]ezra.hartato@poltekba.ac.id, [5]wahyu.anhar@poltekba.ac.id

Abstrak

Pesatnya transformasi digital di berbagai sektor telah membuka peluang besar sekaligus tantangan baru dalam menjaga keamanan informasi. Di tengah upaya pemerintah dan organisasi membangun infrastruktur digital yang kuat, faktor manusia masih menjadi titik lemah yang paling rentan terhadap serangan siber dan kebocoran data. Penelitian ini bertujuan untuk menganalisis tingkat kesadaran keamanan informasi masyarakat dengan mengintegrasikan Human Aspects of Information Security Questionnaire (HAIS-Q) dan Information Security Awareness (ISA) Model sebagai pendekatan mitigasi risiko siber. Model ini menyoroti tiga aspek utama perilaku keamanan digital, yaitu manajemen kata sandi (password management), penggunaan media sosial (social media usage), dan keamanan perangkat seluler (mobile device security), yang menggambarkan dimensi pengetahuan (knowledge), sikap (attitude), dan perilaku (behavior) pengguna. Penelitian ini melibatkan 112 responden aktif pengguna teknologi digital dan dianalisis menggunakan Structural Equation Modeling (SEM) berbasis Partial Least Square (PLS). Integrasi HAIS-Q dan ISA Model dalam penelitian ini memberikan kontribusi konseptual dan praktis untuk meningkatkan literasi keamanan informasi, sekaligus menempatkan pengguna sebagai aktor utama dalam upaya mitigasi risiko siber di era digital.

Kata kunci*— HAIS-Q, Information Security Awareness, Password, Mobile Device, Social Media.*

1. PENDAHULUAN

Saat ini Kementerian Komunikasi dan Informatika telah bertransformasi menjadi Kementerian Komunikasi dan Digital yang memiliki kaitan terhadap perkembangan teknologi digital yang kian masif. Literasi Digital menjadi salah satu pokok bahasan yang saat ini sering terdengar di kalangan generasi muda. Literasi digital merupakan suatu kemampuan yang perlu dimiliki masyarakat dalam menghadapi era digital yang sangat pesat. Hal ini termasuk keterampilan mengakses informasi, berkomunikasi, serta melindungi privasi dan data pribadi dalam lingkungan digital.

Dalam ekspansi literasi digital yang lebih luas tantangan yang dihadapi juga tidak mudah. Melihat data dari Statistik Telekomunikasi Indonesia 2023, Pada tahun 2023, 69,21% penduduk Indonesia telah mengakses internet. Jumlah pelanggan layanan ISP di Indonesia pada tahun 2023 mencapai 13,54 juta pelanggan. Luasnya aktivitas digital yang dilakukan oleh masyrakat, berbanding lurus dengan identitas pribadi yang tersebar di dunia maya.

Banyak ancaman siber yang dihadapi dalam penggunaan layanan digital beberapa diantaranya adalah serangan phishing, malware, dan peretasan data pribadi. Hal ini dipicu oleh kesadaran masyarakat yang tergolong rendah tentang ancaman keamanan siber, sehingga banyak masyarakat yang rentan terhadap penipuan online maupun kebocoran data [1][2][3]. Potensi serangan siber yang terjadi pada transformasi ekonomi digital di Indonesia antara lain, DDoS,

MitM, Phishing, Drive-by-download, Password, SQL Injection, XSS, Eavesdropping, Birthday, and Malware attacks [5]. Puncak dari serangan siber pada infrastruktur digital di Indonesia adalah serangan pada Pusat Data Nasional (PDN) yang melumpuhkan hampir sebagian besar kinerja platform digital pemerintahan. Secara teknis pengelolaan SPBE menjadi tanggung jawab divisi teknologi informasi, tapi ada hal lain yang menjadi penyebab gagalnya keamanan data pada platform digital yang disebabkan oleh faktor non-teknis salah satunya adalah manusia. Saat infrastruktur digital telah di bangun dengan fundamental yang sesuai dengan kaidah utama penerapan keamanan siber, maka manusia atau pengguna infrastruktur digital juga perlu memiliki kesadaran terhadap keamanan informasi digital [4].

Pada tahun 2024 sejumlah serangan siber terjadi di halaman website pemerintahan. PT KAI mengalami serangan siber yang mengakibatkan pencurian lebih dari 22.500 data pelanggan serta data sensitif karyawan. PDN (Pusat Data Nasional) mengalami serangan siber berupa ransomware bernama "Brain Chipper", varian dari "LockBit 3.0". Serangan ini menyebabkan lebih dari 210 instansi pemerintah mengalami gangguan layanan publik, termasuk sektor imigrasi. Selanjutnya, sekitar 4.759.218 data ASN yang dikelola oleh Badan Kepegawaian Negara (BKN) diduga bocor dan ditawarkan di forum hacker. Data yang bocor mencakup nama, tanggal lahir, NIP, nomor SK, jabatan, instansi, alamat, nomor HP, email, pendidikan, dan lainnya. Sekitar 6 juta data Nomor Pokok Wajib Pajak (NPWP) diduga bocor dan diperjualbelikan dengan harga sekitar Rp150 juta.

Infrastruktur Pusat Data Nasional (PDN) menempatkan data pada server di satu tempat yang bertentangan dengan kaidah kemanan informasi digital. Data yang disimpan pada PDN tidak dilakukan backup secara berkala, sehingga proses rollback yang harus dilakukan ketika server PDN diretas mengalami kegagalan muat ulang data. Sederhananya, infrastruktur PDN saat ini belum mencapai kinerja maksimal yang diharapkan untuk suatu server data nasional. Perbaikan telah banyak dilakukan oleh komdigi selaku pemegang akses utama PDN. Beberapa diantaranya peningkatan firewall digital untuk melindungi situs web pemerintahan dan jaringan telekomunikasi, memperluas jaringan *Computer Security Incident Response Team* (CSIRT) yang terintegrasi dan melibatkan berbagai sektor dan mengembangkan AI untuk merespon dan mendeteksi serangan siber. Upaya teknis ini dilakukan untuk memaksimalkan kinerja keamanan data digital. Selain upaya teknis, pemerintah perlu melakukan pemberdayaan pengguna dan peningkatan kesadaran keamanan pada pengguna teknologi digital sebagai aktor utama dan pintu masuk serangan siber.

Human Aspect of Information Security Questionnare (HAIS-Q) merupakan suatu instrumen survey yang digunakan untuk mengukur kesadaran terhadap keamanan informasi. HAIS-Q bertujuan untuk melihat faktor apa yang mempengaruhi kesadaran terhadap keamanan digital dan bagaimana hal ini dapat meningkatkan literasi digital di lingkungan masyarakat Indonesia[7].

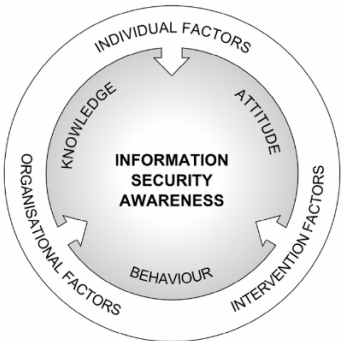
Human Aspect of Information Security Questionnare (HAIS-Q) adalah instrumen yang digunakan untuk mengukur pengetahuan (knowledge), sikap (attitude), perilaku (behavior) yang berkaitan dengan keamanan informasi. HAIS-Q memiliki 7 (tujuh) fokus area yaitu (1) pengelolaan password (*password*), (2) penggunaan surel (e-*mail*), (3) penggunaan internet (internet), (4) penggunaan media sosial (media sosial), (5) perangkat bergerak (*mobile device*), (6) penanganan informasi (information handling), (7) pelaporan insiden (*incident reporting*). HAIS-Q bertujuan untuk mengidentifikasi kesenjangan antara kesadaran keamanan informasi dan perilaku digital [10][11]

Sebuah studi di Indonesia menyatakan bahwa perlu adanya edukasi tentang pemahaman penggunaan kata sandi dan bagaimana cara berbagi informasi digital yang sehat [10]. HAIS-Q digunakan pada penelitian di lembaga keuangan yang menunjukkan bahwa perlu adanya pelatihan edukasi atau literasi digital pada karyawan dengan kesadaran keamanan digital di level menengah [9]. Pada industri skala menengah dilakukan pengukuran kesadaran terhadap keamanan digital yang menyatakan bahwa industri kecil dan menengah memiliki tantangan yang lebih besar

daripada industri besar. Hal ini disebabkan pemahaman terhadap keamanan digital masih sangat rendah [8]

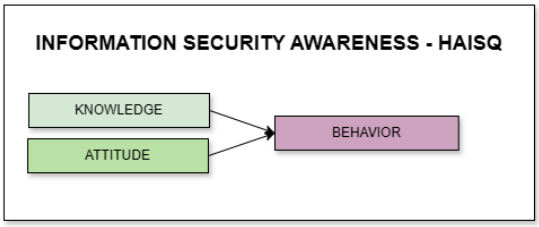
Literasi digital merupakan upaya penting yang perlu dilakukan untuk mengatasi tantangan digital seperti berita palsu (*hoax*) dan keamanan data privasi[13]. Selain mengantisipasi dampak negatif, literasi digital juga dapat digunakan untuk membangun budaya digital yang sehat seperti keterampilan dalam menavigasi dan memanfaatkan teknologi digital secara efektif [14]. Kemampuan penggunaan informasi dan komunikasi yang baik juga menjadi tujuan dalam upaya peningkatan literasi digital [12].

Faktor individu, organisasi dan intervensi pada model ISA mempengaruhi pengetahuan (*knowledge*), sikap (*attitude*) dan perilaku (*behavior*) masyarakat terhadap kesadaraan keamanan informasi. HAIS-Q dapat mendefinisikan pengetahuan *(knowledge)* sebagai referensi terbaik untuk menghadirkan keamanan informasi, sikap *(attitude)* sebagai representasi pandangan terhadap referensi keamanan informasi dan perilaku *(behavior)* sebagai implementasi dari referensi serta pandangan pengguna terhadap keamanan informasi [7].



Gambar 1. Model Information Security Awareness (ISA)

Kata sandi merupakan lapisan pertama pertahanan dalam menjaga keamanan teknologi modern, terutama di era ketika hampir semua aktivitas digital dilakukan melalui perangkat seluler. Kesadaran pengguna dalam membuat, mengelola, dan melindungi kata sandi memiliki peran yang sangat penting dalam menjaga keamanan data pribadi maupun sistem yang digunakan. Penggunaan kata sandi yang kuat dan unik untuk setiap akun bukan hanya bentuk perlindungan teknis, tetapi juga cerminan dari tingkat kesadaran keamanan seseorang. Oleh karena itu, upaya meningkatkan literasi keamanan siber perlu menempatkan kesadaran terhadap pentingnya pengelolaan kata sandi sebagai salah satu fokus utama dalam pendidikan dan kebijakan keamanan informasi, agar setiap individu mampu menjadi benteng pertama dalam menghadapi ancaman dunia digital[15].

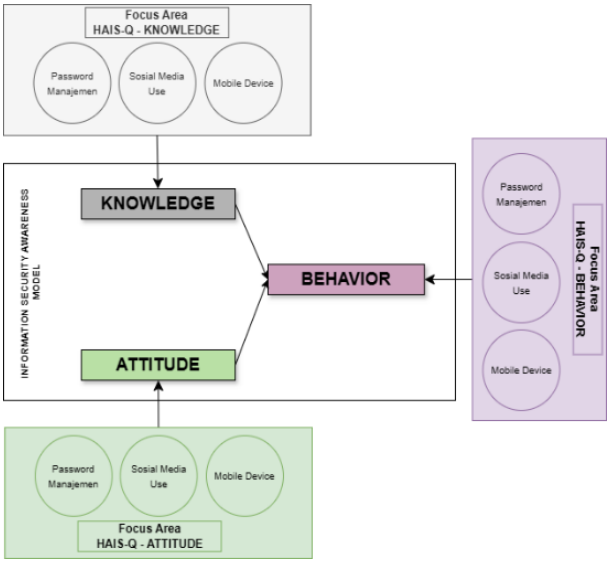


Gambar 2. Model HAIS-Q dan ISA

Dimensi utama yang paling berpengaruh terhadap perilaku keamanan pengguna adalah manajemen kata sandi, penggunaan media sosial, dan keamanan perangkat seluler. Ketiganya saling berkaitan dan membentuk fondasi dari kesiapan keamanan digital seseorang. Pengelolaan kata sandi yang baik seperti membuat kombinasi yang kuat, tidak menggunakan ulang, dan

menggantinya secara berkal menjadi pertahanan pertama terhadap ancaman siber. Di sisi lain, aktivitas di media sosial sering kali menjadi celah bagi penjahat siber untuk melakukan rekayasa sosial melalui informasi pribadi yang dibagikan secara terbuka. Sementara itu, meningkatnya ketergantungan pada perangkat seluler juga memperluas permukaan serangan, karena banyak pengguna yang belum menyadari pentingnya pembaruan sistem, izin aplikasi, dan enkripsi data. Oleh karena itu, tingkat kesadaran terhadap tiga aspek ini mencerminkan seberapa siap seseorang dalam melindungi diri dari risiko dunia maya dan menjadi indikator penting dalam mengukur kesiapan keamanan siber (cybersecurity readiness) pengguna secara keseluruhan [6][15][16].

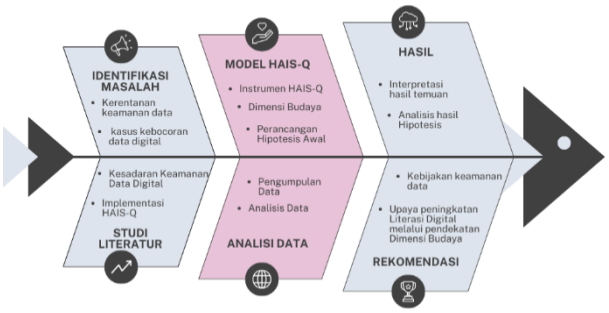
Berdasarkan studi literatur yang telah dilakukan, Instrumen HAIS-Q dapat digunakan untuk merepresentasikan Model ISA dalam konteks keamanan informasi digital yang saat ini menjadi isu utama keamanan informasi di Indonesia. Instrumen HAIS-Q digunakan untuk mengukur knowledge, attitude dan behavior. Aspek yang termasuk pada model penelitian ini adalah (1) password, (2) Social Media, (3) Mobile device [8][9][10].



Gambar 3. Model Penelitian HAIS-Q pada Information Security Model

2. METODE PENELITIAN

Tahapan penelitian yang dilakukan adalah sebagai berikut :



Gambar 4. Diagram Fishbone Penelitian

a. **Identifikasi Masalah :** hal yang dilakukan pada tahap ini adalah melakukan identifikasi kasus yang berkaitan dengan keamanan siber serta serangan yang terjadi 1 tahun terakhir. Dari hasil identifikasi ditemukan beberapa kejadian peretasan terhadap data digital di sejumlah instansi pemerintah yang berakibat pada kebocoran data.
b. **Studi Literatur :** studi literatur dilakukan terhadap kejadian kebocoran data dengan literasi digital yang dimiliki masyarakat terutama di Indonesia. Terdapat satu metode yaitu HAIS-Q yang dapat digunakan untuk melihat tingkat kesadaran masyarakat Indonesia terhadap Keamanan data digital.
c. **Model ISA dan HAIS-Q :** Model Information Security Awareness (ISA) menjadi penting dalam konteks transformasi digital, karena saat ini organisasi banyak mengandalkan platform digital untuk mendukung proses bisnis perusahaannya [16]. Pergeseran ke platform digital memberikan peluang terhadap kejahatan dunia maya yang menargetkan organisasi seperti, pelanggaran data dan penipuan keuangan, yang memerlukan pendekatan proaktif terhadap kesadaran keamanan [1]. HAIS-Q dikembangkan berdasarkan model KAB (Knowledge – Attitude – Behaviour). HAIS-Q merupakan instrumen kuesioner untuk menilai knowledge, attitudes, dan behaviors yang berkaitan dengan keamanan informasi. HAIS-Q digunakan di berbagai konteks, termasuk mobile banking, kesadaran karyawan, dan aspek sosiologis keamanan informasi, dalam mengidentifikasi kerentanan dan meningkatkan praktik keamanan. HAIS-Q bertujuan untuk mengevaluasi faktor manusia terhadap pelanggaran keamanan informasi, dengan fokus pada perilaku (behavior) dan kesadaran pengguna (awareness) [10]. Indikator HAIS-Q yang digunakan dapat dilihat pada Tabel 1.

Tabel 1. Instrumen HAIS-Q

Indikator HAIS-Q	Pertanyaan
Password Management - Knowledge	• Saya mengetahui bahwa saya boleh menggunakan akun dan kata sandi media sosial di akun kerja • Saya mengetahui bahwa membagikan password atau kata sandi akun saya ke rekan kerja diperbolehkan • Yang saya pahami adalah perlunya melakukan kombinasi angka, karakter dan simbol dalam membuat password
Mobile Device - Knowledge	• Ketika bekerja di area publik, saya harus menjaga gadget/smartphone/perangkat digital lainnya untuk tetap berada di dekat saya • Saya dapat mengirimkan data/file pekerjaan yang bersifat rahasia menggunakan jaringan nirkabel (wifi) di fasilitas umum. • Ketika mengerjakan pekerjaan yang sensitif saya harus memastikan bahwa orang lain tidak dapat melihat pekerjaan saya
Social Media - Knowledge	• Saya harus melakukan pengaturan privasi di akun media sosial secara berkala • Saya tidak bisa dipecat dari pekerjaan karena postingan media sosial • Saya dapat memposting atau mengunggah tentang pekerjaan saya di media sosial
Password Management - Attitude	• Saya menggunakan password / kata sandi yang sama untuk akun media sosial dan akun untuk pekerjaan, karena merasa aman • Saya merasa membagikan password / kata sandi akun pekerjaan ke rekan kerja adalah ide yang buruk

	• Saya menggunakan kombinasi karakter, angka dan simbol untuk akun kerja
Mobile Device - Attitude	• Saya merasa ketika bekerja di ruang publik, aman untuk meninggalkan laptop di meja. • Saya merasa mengirimkan data pekerjaan yang bersifat rahasia atau sensitif menggunakan jaringan nirkabel/wifi publik memiliki risiko yang tinggi • Saya merasa, ketika mengakses pekerjaan yang sensitif/rahasia dan dilihat oleh orang lain merupakan hal yang berisiko
Social Media - Attitude	• Saya merasa, ide yang baik untuk secara berkala memeriksa pengaturan privasi akun media sosial saya • Saya merasa tidak masalah jika memposting tentang pekerjaan yang bersifat sensitif atau rahasia di media sosial • Saya merasa berisiko jika memposting informasi tentang pekerjaan di media sosial
Password Management - Behavior	• Saya menggunakan password / kata sandi yang berbeda untuk akun media sosial dan akun pekerjaan • Saya membagikan password / kata sandi akun pekerjaan ke rekan kerja • Saya menggunakan kombinasi karakter, angka dan simbol untuk password atau kata sandi akun kerja
Mobile Device - Behavior	• Ketika bekerja di area publik, saya meninggalkan perangkat teknologi (Laptop/Handphone/Catatan Pekerjaan) meja di ruang terbuka • Saya mengirim data pekerjaan yang sensitif menggunakan jaringan nirkabel/wifi publik • Saya pastikan orang lain tidak dapat melihat layar pekerjaan jika bekerja, yang berkaitan dengan dokumen sensitif
Social Media - Behavior	• Saya tidak pernah memerika pengaturan akun sosial media saya secara berkala • Saya tidak memposting apapun di media sosial sebelum mempertimbangkan konsekuensi atau dampaknya • Saya memposting / mengunggah apapun yang saya inginkan di media sosial.

3. HASIL DAN PEMBAHASAN

Hasil pengumpulan data responden sebanyak 112 responden yang masuk dalam kategori aktif menggunakan teknologi, seperti smartphone, media sosial, WhatsApp, Gmail, dan aplikasi digital lain. Dalam pengumpulan data dapat dilihat bahwa mayoritas responden mengetahui pentingnya kombinasi karakter, angka, dan simbol dalam membuat password, serta menggunakan password yang berbeda antara akun pribadi dan pekerjaan dan hampir semua responden menolak untuk membagikan password kepada rekan kerja dan menyadari risiko jika password digunakan secara sembarangan. Sebagian besar responden sudah menyadari bahwa meninggalkan perangkat (laptop/handphone) di ruang publik tanpa pengawasan adalah tindakan berisiko. Namun, masih ada sebagian kecil responden yang kurang waspada terhadap pengiriman data sensitif melalui jaringan publik (wifi publik). Responden umumnya tidak memposting informasi sensitif tentang pekerjaan di media sosial dan mempertimbangkan dampak sebelum memposting sesuatu. Walau demikian, ada beberapa responden yang masih menganggap remeh penggunaan wifi publik atau pengaturan privasi di media sosial.

SEM adalah metode yang digunakan untuk menguji hipotesis dengan menggunakan Smart-PLS. Kriteria analisis PLS yang diuji terdapat pada tabel berikut :

Tabel 2. Kriteria Model SEM

No	Kriteria	Penjelasan
1	Loading Factor	*loading factor* ≥ 0,4.
2	Cross Loading	Nilai *cross loading* setiap indikator harus lebih besar dari nilai *cross loading* indikator pada konstruk lainnya
3	Composite Reliability	*Composite reliability* ≥ 0,7
4	AVE	Nilai AVE digunakan untuk menjelaskan seberapa baik indikator menjelaskan variabel laten.
5	Latent Construct Correlation	Nilai korelasi antar variabel laten lebih kecil dari nilai akar kuadrat AVE
6	R Square	Nilai *R square* dibagi tiga yaitu Baik jika ≥ 0,67, Moderat jika ≥0,33, dan Lemah jika ≥ 0,19
7	Path Coefficient	Path Coefficient ≤ 0,1 (*Pvalues)*

Berdasarkan hasil pengujian outer model dapat disimpulkan bahwa bahwa indikator-indikator yang membentuk konstruk Knowledge, Attitude, dan Behavior menunjukkan performa pengukuran yang baik.

Tabel 3.Factor Loading Attitude

Indikator	Attitude
MD.A03	0.791
MD.A01	0.801
MD.A02	0.771
PM.A01	**0.778**
PM.A02	**0.696**
PM.A03	**0.782**
SM.A01	**0.821**
SM.A02	**0.840**
SM.A03	**0.755**

Nilai tersebut menunjukkan bahwa setiap indikator mampu menjelaskan konstruknya dengan validitas yang kuat. Batas minimal loading faktor yang disarankan adalah ≥ 0,70 [19], sehingga indikator yang berada di atas nilai ini dapat dinyatakan valid.

Tabel 4. Factor Loading Behavior

Indikator	Attitude
MD.B01	0.804
MD.B02	0.828
MD.B03	0.838
PM.B01	0.782
PM.B02	0.769
PM.B03	0.771
SM.B01	0.637
SM.B02	0.792
SM.B03	0.755

Meskipun terdapat beberapa indikator dengan nilai mendekati batas minimal, seperti 0,707; 0,717; dan 0,755, indikator-indikator tersebut masih dapat diterima karena termasuk dalam kategori moderate loading dan tetap memberikan kontribusi signifikan terhadap konstruk yang diukur. Dengan demikian, seluruh indikator pada penelitian ini tidak perlu dieliminasi karena sudah memenuhi kriteria convergent validity.

Tabel 5. Factor Loading Knowledge

Indikator	Attitude
MD.K01	0.817
MD.K02	0.839
MD.K03	0.814
PM.K01	0.707
PM.K02	0.760
PM.K03	0.764
SM.K01	0.760
SM.K02	0.784
SM.K03	0.834

Selain itu, hasil ini juga mengindikasikan bahwa masing-masing indikator lebih merefleksikan konstruk yang dituju dibandingkan konstruk lainnya, sehingga discriminant validity juga terpenuhi. Secara keseluruhan, outer model yang diperoleh menunjukkan kualitas pengukuran yang baik dan reliabel, sehingga dapat digunakan untuk menguji inner model lebih lanjut dengan tingkat kepercayaan yang tinggi.

Hasil pengujian inner model menunjukkan bahwa hubungan antarvariabel laten dalam penelitian ini terkonfirmasi signifikan [19]. Konstruk Knowledge berpengaruh positif terhadap Behavior dengan nilai koefisien jalur sebesar 0,366, T-statistik > 1,96, dan P-value < 0,05. Hal ini mengindikasikan bahwa pengetahuan yang lebih tinggi secara signifikan dapat meningkatkan perilaku individu sesuai arah pengaruh pengetahuan dalam memahami risiko siber dalam perilaku digital.

Tabel 6. Inner Model

Konstruk	Koefisien Jalur	T-Statistics	P Values
ATTITUDE -> BEHAVIOR	0.551	8.523	0.000
KNOWLEDGE -> BEHAVIOR	0.366	5.009	0.000

Sementara itu, konstruk Attitude memiliki pengaruh yang lebih dominan terhadap Behavior, dengan nilai koefisien jalur sebesar 0,551, T-statistik > 1,96, dan P-value < 0,01. Temuan ini menegaskan bahwa sikap individu merupakan faktor yang paling kuat dan signifikan dalam memengaruhi perilaku.

Tabel 7. Outer Model

Konstruk	R Square
Behavior	0.781

Nilai R^2 pada konstruk Behavior sebesar 0,781 menunjukkan bahwa 78,1% varians perilaku dapat dijelaskan oleh pengetahuan dan sikap, sedangkan sisanya 21,9% dipengaruhi oleh faktor lain di luar model. Nilai $R^2 > 0,67$ dikategorikan kuat, sehingga dapat disimpulkan bahwa model struktural yang digunakan memiliki kemampuan prediktif yang sangat baik [19].

4. KESIMPULAN

Temuan ini mendukung argumentasi teoretis bahwa perubahan perilaku lebih efektif dicapai melalui pembentukan sikap positif dibandingkan hanya dengan peningkatan pengetahuan. Dengan demikian, hasil penelitian ini memperkuat literatur sebelumnya yang menekankan peranan dominan sikap dalam membentuk perilaku, sekaligus menegaskan pentingnya intervensi berbasis sikap dalam strategi peningkatan perilaku positif. Pengetahuan dan sikap yang dimiliki suatu individu akan mempengaruhi perilaku digital. Kesadaran inidividu tentang risiko dan bagaimana berinteraksi digital dapat meningkatkan perilaku digital yang lebih positif dan menjaga privasi. Hasil penelitian ini memberikan kontribusi terhadap pengembangan teori perilaku dengan menegaskan bahwa sikap (Attitude) memiliki peranan yang lebih dominan dibandingkan pengetahuan (Knowledge) dalam memengaruhi perilaku (Behavior). Temuan ini konsisten dengan model-model perilaku klasik, seperti Theory of Planned Behavior [18] yang menempatkan sikap sebagai determinan utama dalam pembentukan perilaku. Dengan nilai koefisien jalur yang signifikan dan R^2 yang kuat, penelitian ini memperkuat literatur empiris bahwa intervensi teoretis yang menitikberatkan pada penguatan sikap lebih relevan dalam menjelaskan perilaku individu. Selain itu, hasil ini juga memberikan bukti empiris bagi penerapan Structural Equation Modeling berbasis PLS-SEM dalam menguji hubungan laten dengan prediktivitas yang tinggi, sehingga memperkaya khasanah metodologis pada penelitian bidang perilaku.

Dari sisi praktis, hasil penelitian ini menunjukkan bahwa strategi peningkatan perilaku positif tidak cukup hanya dengan meningkatkan pengetahuan, melainkan perlu diiringi dengan pembentukan dan penguatan sikap yang mendukung. Misalnya, dalam konteks pendidikan, program pembelajaran sebaiknya tidak hanya berfokus pada transfer pengetahuan, tetapi juga pada pembentukan nilai, keyakinan, dan sikap positif peserta didik. Dalam konteks organisasi, hasil ini dapat menjadi dasar bagi manajer atau pembuat kebijakan untuk merancang pelatihan yang menekankan aspek sikap, seperti motivasi, komitmen, dan kesadaran etis, sehingga berdampak lebih signifikan pada perubahan perilaku karyawan. Dengan demikian, implikasi praktis dari penelitian ini menekankan pentingnya pendekatan yang holistik, yaitu menggabungkan peningkatan pengetahuan dan pembentukan sikap, dengan prioritas yang lebih besar pada dimensi sikap.

5. SARAN

Penelitian lebih lanjut dapat menerapkan instrument HAISQ secara keseluruhan untuk melihat perbedaan kesadaran keamanan informasi pada organisasi swasta dan organisasi publik.

UCAPAN TERIMA KASIH

Ucapan terima kasih kepada Politeknik Negeri Balikpapan yang telah mendukung terlaksananya penelitian ini

DAFTAR PUSTAKA

[1] Undale, P. S., & Shinde, V. (2024). Digital transformation and cyber security: unveiling awareness. Towards Excellence, 84–91. https://doi.org/10.37867/te160207

[2] Tikanmäki, I., & Ruoslahti, H. (2024). Human Factors Make or Break Cybersecurity! Information & Security: An International Journal, 55(3), 245–259. https://doi.org/10.11610/isij.5522

[3] Saleem, M., Kumar, R., Chawla, C., & Singh, M. (2024). Understanding the Human Factors in the Psychology of Cyber Threats. Advances in Human and Social Aspects of Technology Book Series, 39–52. https://doi.org/10.4018/979-8-3693-9235-5.ch003

[4] Ramadhani, E. H., Enriko, I. K. A., & Puspita Sari, E. L. I. (2025). Kajian Strategik Manajemen Keamanan Siber terhadap Proyek Telematika di Indonesia: Studi Kasus Kebocoran Pusat Data Nasional. Jurnal Indonesia : Manajemen Informatika Dan Komunikasi, 6(1), 570–580. https://doi.org/10.35870/jimik.v6i1.1210

[5] Tatara, B. A., Abdurachman, B., Mustofa, D. L., & Yacobus, D. (2023). The Potential of Cyber Attacks in Indonesia's Digital Economy Transformation. Nuansa. https://doi.org/10.19105/nuansa.v20i1.7362

[6] Collier, H., Morton, C., & Alharthi, D. (2023). Cultural Influences on Information Security. 22(1), 143–150. https://doi.org/10.34190/eccws.22.1.1127

[7] Riahi, E., & Islam, M. S. (2024). Employees' information security awareness (ISA) in public organisations: insights from cross-cultural studies in Sweden, France, and Tunisia. https://doi.org/10.1080/0144929x.2024.2311734

[8] Papp, G., & Lovaas, P. (2021). Assessing Small Institutions' Cyber Security Awareness Using Human Aspects of Information Security Questionnaire (HAIS-Q) (pp. 933–948). Springer, Cham. https://doi.org/10.1007/978-3-030-80129-8_62

[9] Styoutomo, Y. A., & Ruldeviyani, Y. (2023). Information Security Awareness Raising Strategy Using Fuzzy AHP Method with HAIS-Q and ISO/IEC 27001:2013: A Case Study of XYZ Financial Institution. Teaching Anthropology. https://doi.org/10.21512/commit.v17i2.8272

[10] Anastasiah, M., & Pandia, H. (2024). Analisis Perilaku Pengguna Mobile Banking Terhadap Keamanan Informasi Menggunakan Metode Human Aspects of Information Security Questionnaire (HAIS-Q). https://doi.org/10.31004/innovative.v4i2.9684

[11] Hakim, L. F. (2025). Insider Threats: The Cybersecurity Analysis using OCTAVE Allegro which are combined with HAIS-Q. Deleted Journal, 3(1), 36–47. https://doi.org/10.61132/uranus.v3i1.649

[12] Wiguna, I. W. D. P., & Sudarti, N. W. (2024). Peran Literasi Digital dalam Penguatan Profil Pelajar Pancasila Dimensi Mandiri, Bernalar Kritis, dan Kreatif. 1(1), 122–132. https://doi.org/10.62951/prosemnasipi.v1i1.15

[13] Parra, J. B., Niebles, W., & Ruiz, C. P. (2024). Digital Literacy: A Strategy for Leveraging Skills Development. Evolutionary Studies in Imaginative Culture. https://doi.org/10.70082/esiculture.vi.1617

[14] Alfiani, A., Azraf, A., & Kamal, M. M. (2024). Literasi Digital : Solusi Tantangan Dan Peluang Komunikasi Sosial Di Era Digital. 1(3), 98–101. https://doi.org/10.62523/kalijaga.v1i3.17

[15] Hakim, L. F. (2025). Insider Threats: The Cybersecurity Analysis using OCTAVE Allegro which are combined with HAIS-Q. Deleted Journal, 3(1), 36–47. https://doi.org/10.61132/uranus.v3i1.649

[16] Mai, N., & Tick, J. (2021). Cyber Security Awareness and Behavior of Youth in Smartphone Usage: A Comparative Study between University Students in Hungary and Vietnam. Acta Polytechnica Hungarica, 18(2), 115–132.

[17] H. Taherdoost, S. Sahibuddin, and N. Jalaliyoon, "An empirical study on information security awareness: Password, social media, and mobile device security practices," *International Journal of Network Security & Its Applications (IJNSA)*, vol. 13, no. 3, pp. 15–32, 2021, doi: 10.5121/ijnsa.2021.13302.

[18] A. Alotaibi, R. Aljazzaf, F. Alotaibi, and A. Alzahrani, "A systematic literature review of cybersecurity scales," *Heliyon*, vol. 9, no. 7, e16441, 2023, doi: 10.1016/j.heliyon.2023.e16441.

[19] I. Ajzen. (1991) "The theory of planned behavior," Organizational Behavior and Human Decision Processes, vol. 50, no. 2, pp. 179–211. doi: 10.1016/0749-5978(91)90020-T.

[20] F. Hair Jr, J., Sarstedt, M., Hopkins, L., & G. Kuppelwieser, V. (2014). Partial least squares structural equation modeling (PLS-SEM) An emerging tool in business research. European business review, 26(2), 106-121.