Sistemasi: Jurnal Sistem Informasi
Volume 15, Nomor 4, 2026: 1398-1408
ISSN:2302-8149
e-ISSN:2540-9719

Analisis Kesadaran Keamanan Informasi Pegawai: Studi Kasus Pusinfowas BPKP

Analysis of Government Employees' Information Security Awareness: A Case Study of Pusinfowas BPKP

[1]Basrah Nasution*, [2]Setiadi Yazid, [3]Yudho Giri Sucahyo
[1,2,3]Fakultas Ilmu Komputer, Universitas Indonesia
[1,2,3]Jl. Salemba Raya No.4, Jakarta Pusat
*e-mail: basrah.nasution@ui.ac.id

(***received*:** 31 March 2026, ***revised*:** 8 April 2026, ***accepted*:** 9 April 2026)

Abstrak

Pemanfaatan teknologi informasi sebagai alat yang dipercaya dapat memudahkan proses bisnis dalam organisasi tidak lepas dari tantangan ancaman terhadap keamanan informasi. Berdasarkan laporan BSSN terkait insiden siber pada tahun 2024, tren ancaman berupa *data exposure* sebesar 58,34% berasal dari sektor administrasi pemerintah. Manusia merupakan bagian paling lemah dalam keamanan, upaya utama dalam memperbaiki keamanan dapat dimulai dengan pengukuran tingkat kesadaran keamanan. Dari sekian banyak unit kerja BPKP, Pusinfowas sebagai pusat pengelolaan TI selayaknya menjadi sample pengujian dan membawa yang lainnya kearah tingkat kesadaran keamanan informasi terbaik. Studi penelitian ini menggunakan metodel HAIS-Q untuk mengukur tingkat kesadaran kemanan informasi pegawai Pusinfowas. HAIS-Q terdiri dari tiga dimensi yaitu *knowledge*, *attitude*, *behavior* dan tujuh fokus area yaitu *password management*, *email use*, *internet use*, *social media use*, *mobile device use*, *information handling*, dan *incident reporting* Hasil penelitian menunjukkan bahwa level kesadaran keamanan informasi pegawai berada pada level "Baik" dengan rentang nilai 80%-100% pada setiap dimensi dan fokus area pada model HAIS-Q.

Kata kunci: pemerintah, HAIS-Q, kesadaran keamanan informasi, teknologi informasi

Abstract

The utilization of information technology as a tool that is widely believed to facilitate business processes within organizations is inseparable from challenges related to information security threats. According to the 2024 cyber incident report issued by the National Cyber and Crypto Agency (BSSN), data exposure threats accounted for 58.34%, with most incidents originating from the government administration sector. Humans are considered the weakest link in information security; therefore, the primary effort to improve security can begin with measuring the level of security awareness. Among the various work units within BPKP, Pusinfowas, as the central information technology management unit, is considered an appropriate sample for evaluation and is expected to contribute to improving information security awareness across other units. This study employs the Human Aspects of Information Security Questionnaire (HAIS-Q) model to measure the level of information security awareness among employees at Pusinfowas. The HAIS-Q model consists of three dimensions—knowledge, attitude, and behavior—and seven focus areas: password management, email use, internet use, social media use, mobile device use, information handling, and incident reporting. The results indicate that employees' information security awareness is at a "Good" level, with scores ranging between 80% and 100% across all HAIS-Q dimensions and focus areas.

***Keywords:** : government, HAIS-Q, information security awareness, information technology*

1 Pendahuluan

Pemanfaatan teknologi informasi di era transformasi digital saat ini sesuatu yang berkembang pesat di ruang lingkup pemerintahan di Indonesia. Badan Pengawasan Keuangan dan Pembangunan (BPKP) termasuk instansi pemerintah yang aktif berinovasi dengan melibatkan teknologi informasi sebagai alat pendorong jalannya proses bisnis yang lebih efektif dan efisien [1]. Penggunaan teknologi

 ISSN:2302-8149
e-ISSN:2540-9719

informasi yang semakin masif tidak selamanya berjalan mulus, selalu ada berbagai tantangan dalam penerapannya. Salah satu tantangan yang banyak menarik perhatian publik adalah masalah keamanan informasi (*information security*) dari aspek manusia [2].

Berdasarkan laporan BSSN terkait rekapitulasi dugaan insiden siber berdasarkan sektor pada tahun 2024, administrasi pemerintahan merupakan sektor dengan dugaan insiden siber paling tinggi [3]. Selain itu, dalam laporannya BSSN juga menjelaskan bahwa sektor administrasi pemerintahan merupakan sektor dengan *data exposure* tertinggi. Ditemukan 56.128.160 *data exposure* sepanjang tahun 2024, 58,34% dari keseluruhan *data exposure* berasal dari sektor administrasi pemerintahan, 3,58% sektor keuangan, 2,73% sektor TIK, 2,70 sektor transportasi, 1,88% sektor ESDM, 0,34 sektor kesehatan, 0,19 sektor pangan, 0,11 sektor pertahanan dan 30,14% sektor lainnya.

Badan Pengawas Keuangan dan Pembangunan (BPKP), melalui Pusat Informasi Pengawasan (Pusinfowas) secara aktif memantau ancaman serangan siber setiap bulan. Sebagai upaya untuk menangkal serangan siber, BPKP menerapkan perangkat keamanan seperti *firewall*, perangkat lunak antivirus, WAF, dan lainnya. Dalam laporan pemantauan manajemen dan operasional keamanan TI BPKP menunjukkan bahwa risiko akses tidak sah, serangan siber, dan kerentanan teknis berada pada tingkat probabilitas tinggi [4]. Selain menerapkan berbagai perangkat teknologi keamanan informasi, BPKP juga aktif memberikan himbauan kepada pegawai untuk melakukan pergantian *password* secara berkala. Upaya ini dilakukan secara periodik melalui intervensi pada sistem informasi yang digunakan, dimana sistem akan mengingatkan pengguna untuk mengganti *password* secara berkala. Himbauan secara tertulis juga dilakukan melalui surat pemberitahuan kepada seluruh pegawai.

Berbagai upaya peningkatan keamanan yang dilakukan membutuhkan kesadaran pegawai dalam mematuhi arahan keamanan informasi yang disampaikan. Keamanan informasi umumnya diatur oleh serangkaian aturan formal yang dibuat oleh organisasi, yang terdiri dari praktik dan protokol yang berlaku, seperti menjaga kerahasiaan kata sandi, melaporkan insiden keamanan, menggunakan jaringan internal selama bekerja, dan sebagainya [5]. Kesadaran keamanan informasi merupakan proses yang dinamis, dan semakin sulit seiring dengan terus berubahnya risiko. Oleh karena itu, pengukuran kesadaran keamanan informasi sangat diperlukan untuk memastikan keberlanjutan organisasi dalam menghadapi tantangan risiko keamanan informasi yang terus berkembang. Kesadaran keamanan informasi merupakan salah satu faktor kunci dalam meningkatkan keamanan informasi di tempat kerja [6].

Sejauh ini, belum pernah dilakukan asesmen secara sistematis mengenai tingkat kesadaran keamanan informasi di lingkungan kerja Badan Pengawasan Keuangan dan Pembangunan (BPKP). Oleh karena itu, penelitian ini bertujuan untuk memperoleh pemahaman yang lebih komprehensif mengenai tingkat kesadaran keamanan informasi di lingkungan kerja BPKP sebagai salah satu organisasi pemerintah yang memiliki peran strategis dalam pengawasan keuangan dan pembangunan nasional. Dalam penelitian ini, proses pengujian dilakukan terhadap pegawai yang berada di lingkungan unit kerja Pusat Informasi Pengawasan (Pusinfowas). Unit kerja tersebut merupakan pusat pengelolaan teknologi informasi di BPKP yang memiliki tanggung jawab dalam penyediaan, pengembangan, serta pengelolaan infrastruktur dan layanan sistem informasi organisasi. Sebagai unit kerja yang berfungsi sebagai pusat teknologi informasi, Pusinfowas memiliki peran yang sangat krusial dalam memastikan bahwa pengelolaan informasi dan sistem informasi dilakukan secara aman dan andal. Oleh karena itu, Pusinfowas memiliki prioritas tinggi untuk diuji terlebih dahulu kesadaran keamanan informasi pegawainya sebelum hal yang sama diterapkan pada unit kerja lainnya.

Berdasarkan latar belakang tersebut, penelitian ini difokuskan untuk menjawab pertanyaan penelitian, yaitu: “Bagaimana tingkat kesadaran keamanan informasi pegawai di lingkungan Pusinfowas BPKP?” Pertanyaan ini menjadi penting karena pemahaman mengenai tingkat kesadaran keamanan informasi pegawai dapat memberikan gambaran mengenai kesiapan organisasi dalam menghadapi berbagai ancaman keamanan informasi yang semakin kompleks. hasil dari penelitian ini diharapkan dapat menjadi landasan berpikir bagi organisasi dalam merumuskan kebijakan, strategi, maupun program peningkatan kesadaran keamanan informasi secara lebih terarah dan efektif. Dengan adanya pemahaman yang lebih baik mengenai tingkat kesadaran keamanan informasi pegawai, organisasi dapat merancang berbagai inisiatif seperti pelatihan, sosialisasi, maupun penguatan kebijakan keamanan informasi yang lebih sesuai dengan kebutuhan organisasi, sehingga pada akhirnya dapat meningkatkan tingkat keamanan informasi secara keseluruhan di lingkungan BPKP.

 ISSN:2302-8149
e-ISSN:2540-9719

2 Tinjauan Literatur

Kesadaran keamanan informasi adalah bentuk penilaian seseorang dalam memahami, berkomitment, dan bertindak sesuai dengan aturan atau panduan keamanan informasi dan aturan-aturan yang berlaku [7]. Kesadaran keamanan informasi merupakan proses yang dinamis karena ancaman dan risiko keamanan informasi terus berkembang seiring dengan kemajuan teknologi informasi. Oleh karena itu, organisasi perlu melakukan pengukuran tingkat kesadaran keamanan informasi secara berkala guna memastikan kesiapan organisasi dalam menghadapi perubahan risiko keamanan serta menjaga keberlangsungan operasional organisasi [8]. Terdapat beberapa penelitian terdahulu dengan fokus pengukuran kesadaran keamanan informasi dengan objek berbeda-beda.

Rosihan and Hidayanto mengukur tingkat kesadaran keamanan informasi pegawai dan memberikan rekomendasi untuk peningkatan kesadaran (*awareness*) pada Direktorat Jenderal Pemasyarakatan (Ditjen PAS) Kementerian Hukum dan Ham (Kemenkumham) [9]. Penelitian menggunakan instrumen HAIS-Q (*Human Aspect of Information Security Questionnaire*) dan Indeks KAMI (Keamanan Informasi). Terdapat 9 fokus area yang diuji pada kuesioner penelitian mencakup *Password Management*, *Email Usage*, *Internet Usage*, *Social Media*, *Mobile Device*, *Information Handling*, *Incident Reporting*, *Information Security Policy*, dan *Workstation Security*. Hasil penelitian menunjukkan bahwa tingkat kesadaran keamanan informasi pegawai berada pada kategori baik, namun beberapa fokus area seperti *Incident Reporting* dan *Internet Usage* masih memerlukan perhatian lebih melalui peningkatan kebijakan, penerapan sanksi, serta penguatan program pelatihan guna menjaga dan meningkatkan keamanan informasi di lingkungan organisasi.

Penelitian dari sektor institusi negara lainnya dilakukan oleh Effendy dkk. Penelitian Effendy dkk mengukur tingkat kesadaran keamanan informasi pegawai pada Politeknik XYZ [10]. Studi ini menggunakan dimensi KAB (*knowledge-attitude-behavior*) dan fokus area HAIS-Q sebagai landasan pengukuran serta melakukan kustomisasi pembobotan pada masing-masing fokus area dengan metode AHP (*Analytical Hierarchy Process*). Hasil penelitian menunjukkan skor kesadaran keamanan informasi pegawai Politeknik XYZ keseluruhan berada pada tingkat menegah dengan skor 66,5%. Fokus area *social media use* adalah fokus area dengan skor terendah pada studi ini, yaitu dengan skor 60,9%. Temuan penelitian ini mengindikasikan urgensi tindakan peningkatan kesadaran keamanan informasi pegawai pada Politeknik XYZ. Kedua penelitian ini menunjukkan keberhasilan dalam melakukan pengukuran kesadaran keamanan informasi dari sektor institusi atau lembaga negara.

Penelitian terdahulu juga menunjukkan keberhasilan pengukuran kesadara keamanan informasi pada pegawai korporasi atau perusahaan. Shakti dan Hidayanto mengukur tingkat kesadaran keamanan informasi pegawai pada sebuah lembaga keuangan PT XYZ [11]. Penelitian menerapakan metode kuantitatif untuk menghitung tingkat kesadaran keamanan informasi pegawai. Kerangka penelitian ini menggunakan dimensi KAB dan fokus area HAIS-Q ditambah satu fokus area merujuk kepada indeks KAMI. Pembobotan masing-masing dimensi dan fokus area dilakukan dengan pendekatan AHP. Sebanyak 52 responden terlibat dalam penelitian ini. Hasil penelitian menunjukkan bahwa pegawai PT XYZ memiliki tingkat kesadaran keamanan informasi yang tergolong baik, sehingga pada kondisi saat ini belum diperlukan tindakan perbaikan yang bersifat mendesak. Meskipun demikian, masih terdapat beberapa area yang berpotensi untuk ditingkatkan. Oleh karena itu, penelitian ini memberikan sejumlah rekomendasi sebagai upaya untuk meningkatkan sekaligus mempertahankan tingkat kesadaran keamanan informasi di kalangan pegawai.

Penelitian dengan objek pegawai perusahaan lainnya dilakukan Kritzinger dkk. Peneliti mengidentifikasi level kesadaran keamanan informasi di Afrika Selatan, dengan objek berupa karyawan dari beberapa perusahaan [12]. Penelitian ini menggunakan instrumen penelitian berupa kuesioner dengan merujuk pada model HAIS-Q, analisis data dilakukan secara statistik deskriptif untuk mengetahui skor pada masing-masing fokus area HAIS-Q. Selain itu dilakuan juga analisis dengan uji t-test dan ANOVA untuk mengidentifikasi perbedaan signifikan antar kelompok demografis. Hasil penelitian menunjukkan bahwa faktor usia, bahasa, ukuran organisasi, dan gender perlu dipertimbangkan dalam perancangan, pengembangan, maupun pembaruan program kesadaran keamanan informasi di organisasi. Penelitian ini juga memberikan rekomendasi untuk mengatasi faktor-faktor tersebut serta mengidentifikasi tiga area yang menjadi perhatian terkait keamanan informasi dan perilaku karyawan, yaitu penggunaan internet yang aman, penggunaan email yang aman, dan penggunaan media sosial di lingkungan kerja.

 ISSN:2302-8149
e-ISSN:2540-9719

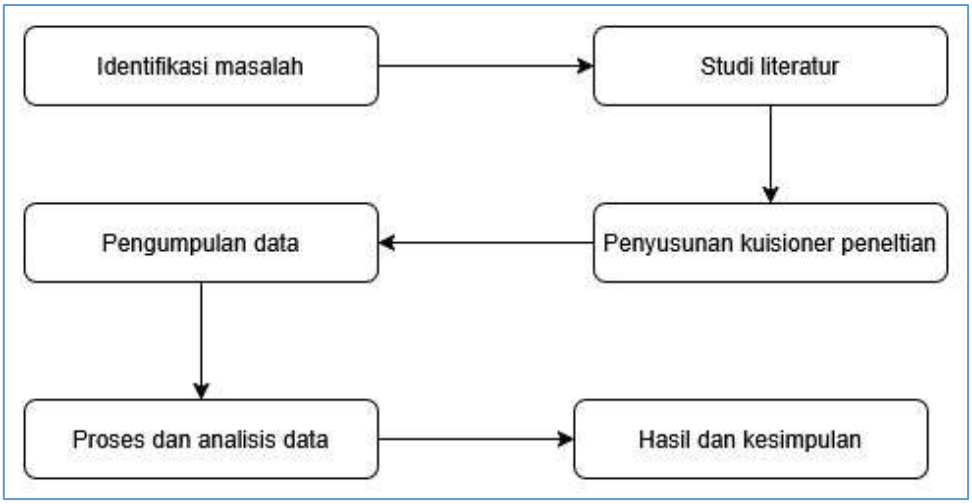
Pengukuran kesadaran keamanan informasi tidak hanya mencakup lingkup lembaga negara atau korporasi, namun juga dapat diterapkan pada objek masyarakat umum seperti penelitian pengukuran tingkat kesadaran keamanan informasi pada pengguna aplikasi kesehatan Alodokter di Indonesia yang dilakukan Atlanta dkk [13]. Penelitian ini menggunakan model HAIS-Q dengan dimensi KAB dalam pengukuran tingkat kesadaran keamanan informasi pengguna aplikasi. Penelitian ini menunjukkan bahwa tingkat kesadaran keamanan informasi pengguna aplikasi Alodokter di Indonesia berada pada kategori baik dengan nilai sebesar 95,5%. Namun demikian, dari sudut pandang dimensi, ditemukan dimensi pengetahuan memperoleh skor terendah, terutama terkait pelaporan insiden keamanan informasi serta kebiasaan memeriksa email menggunakan jaringan Wi-Fi gratis yang berpotensi mengancam keamanan data pribadi. Dari sisi fokus area, aspek *information handling* juga menunjukkan skor rendah, khususnya terkait pengaturan *screensaver* untuk mencegah akses tidak sah ke perangkat pribadi, serta kebiasaan pengguna yang belum rutin mengganti kata sandi.

Berdasarkan penelitian sebelumnya pengukuran tingkat kesadaran keamanan informasi masih didominasi oleh model HAIS-Q. Pada tahun 2006, Kruger dan Kearney mengembangkan model pengetahuan, sikap, dan perilaku, yang dikenal sebagai Model KAB. Kemudian, pada tahun 2013, Parsons dkk. mengembangkan model *Human Aspect of Information Security* (HAIS) dalam bentuk kuesioner dengan 7 fokus area, yang merupakan perluasan dari model KAB. Fokus area pada model HAIS-Q mencakup *Password Management, Email Use, Internet Use, Social Media Use, Mobile Device Use, Information Handling,* dan *Incident Reporting.* Sejalan dengan tren tersebut, penelitian ini akan menerapkan model HAIS-Q dengan dimensi KAB untuk mengukur kesadaran keamanan informasi pegawai pada unit kerja Pusinfowas BPKP.

3 Metode Penelitian

3.1 Alur Penelitian

Penelitian ini dilakukan dengan enam tahapan proses seperti dijelaskan pada Gambar 1. Tahap pertama yaitu identifikasi masalah pada instansi yang diteliti. Pada tahap ini dilakukan pengamatan data-data pendukung dan wawancara degan pemangku kepentingan organisasi. Hasil dari identifikasi masalah dijadikan sebagai masukan untuk bahan penelitian. Selanjutnya dilakukan studi literatur untuk menemukan model pengukuran kesadaran keamanan informasi. Dilakukan perbandingan dengan penelitian terdahulu serta dilakukan penelusuran rujukan akademis untuk mendukung landasan teori penelitian. Kemudian disusun instrumen penelitian berupa kuesioner mengikuti model HAIS-Q. Hasil kuesioner diolah dan dianalisis untuk menyusun hasil peneltian. Pada tahap akhir hasil penelitian disajikan beserta kesimpulan dan saran.



Gambar 1 Alur penelitian

3.2 Instrumen Penelitian

Instrumen penelitian berupa kuesioner. Kuesioner terdiri dari 45 pertanyaan yang dibagi ke dalam tiga bagian mengikuti model HAIS-Q guna mengukur *knowledge*, *attitude*, dan *behavior* dari responden. Pertanyaan juga didesain berdasarkan tujuh fokus area dari model HAIS-Q. Kuesioner

 ISSN:2302-8149
e-ISSN:2540-9719

didesain mengunakan 5 poin skala likert dimulai dari 1 (sangat tidak setuju), 2 (tidak setuju), 3 (kurang setuju), 4(setuju), 5(sangat setuju). Kuesioner dibagikan kepada responden dalam bentuk formulir daring dengan menggunakan *google form*.

3.3 Prosedur Pengumpulan Data

Penelitian dilakukan dengan target responden adalah pegawai Pusinfowas BPKP. Penelitian dilakukan pada bulan Mei 2025. Kuesioner dibagikan kepada 79 pegawai yang merupakan populasi pada lingkup penelitian ini. Untuk menentukan jumlah sample yang dibutuhkan digunakan rumus slovin [14] seperti pada rumus (1) dengan *margin of error* sebesar 5%:

$$n = \frac{N}{1 + N(e)^2} \quad (1)$$

Keterangan:
n = Ukuran sample/jumlah responden =66

N= Jumlah populasi = 79

e = tingkat kesalahan *(margin of error)* =0,05

Berdasarkan perhitungan diatas dibutuhkan 66 orang responden dalam penelitian. Berdasarkan hasil pengisian kuesioner, terdapat 68 data yang berhasil terkumpul. Sehingga jumlah responden dinilai cukup untuk melakukan analisis data pada tahap selanjutnya. Setelah data terkumpul, selanjutnya dilakukan perhitungan indeks persentase pada masing-masing fokus area dengan rumus (2), dimana total skor pada skala likert dibagi dengan Y. Pada rumus tersebut Y adalah maksimal skor pada skala likert dikali dengan jumlah responden.

$$Index\ \% = \frac{Total\ Score}{Y} \quad (2)$$

Hasil assessment diklasifikasikan kedalam tiga level kesadaran keamanan informasi mengikuti metode yang dikembangkan oleh Kruger dan Kearney. Nilai presentase 80-100% masuk pada level baik(*good*), 60-79 masuk pada level sedang (*medium*), dan nilai 0-59% masuk pada level terendah (*low*). Ketiga level tersebut dipetakan sebagaimana ditunjukkan pada Tabel 1.

Tabel 1 Level Kesadaran keamanan informasi

Level	Persentase Pengukuran (%)
Good	80-100
Medium	60-79
Low	0-59

Bobot pada masing-masing dimensi KAB merujuk pada penelitian Kruger dan Kearney seperti dijelaskan pada Tabel 2. Bobot *behavior* memiliki nilai tertinggi dibandingkan dua dimensi lainnya. Hal tersebut merujuk kepada sudut pandang psikologi yang menjadi landasan model KAB, dimana sikap (*attitude*) dan pengetahuan (*knowledge*) seseorang tidak akan memberikan dampak apapun terhadap keamanan apabila tidak diwujudkan dalam perilaku (*behavior*) yang aman [15].

Tabel 2 Bobot dimensi

Dimensi	Bobot
Knowledge	30%
Attitude	20%
Behavior	50%

 ISSN:2302-8149
e-ISSN:2540-9719

3.4 Uji Validitas dan Reliabilitas

Uji validitas dan reliabilitas dilakukan untuk memastikan bahwa instrumen penelitian akurat dan konsisten dalam mengukur konstruk yang dibangun. Uji validitas bertujuan untuk memeriksa apakah setiap butir kuesioner secara tepat mewakili dimensi pengetahuan, sikap, dan perilaku sebagaimana didefinisikan dalam model HAIS-Q. Validitas isi dipastikan melalui pengembangan butir-butir yang cermat berdasarkan area fokus HAIS-Q yang telah ditetapkan, sehingga menyelaraskan pertanyaan dengan konsep teoritis yang relevan tentang kesadaran keamanan informasi. Selain itu, validitas konstruk dinilai secara statistik dengan menganalisis korelasi antara setiap butir dan skor totalnya, di mana butir-butir dengan nilai korelasi yang melebihi ambang batas sesuai koefisien korelasi Pearson yang diterima dianggap valid dan sesuai untuk analisis lebih lanjut.

Pengujian realibilitas bertujuan untuk mengetahui sejauh mana instrumen atau alat ukur yang digunakan memberikan hasil yang konsisten dan stabil jika diukur berulang kali dalam kondisi yang sama [16]. Pengukuran realibilitas pada penelitian ini menggunakan koefisien Cronbach's Alpha, yang merupakan salah satu teknik pengujian reliabilitas yang paling umum digunakan dalam penelitian sosial dan perilaku. Metode ini digunakan untuk mengukur tingkat konsistensi internal dari sejumlah butir pertanyaan dalam suatu skala pengukuran. Nilai koefisien Cronbach's Alpha berada pada rentang 0 hingga 1, di mana semakin tinggi nilai koefisien yang diperoleh menunjukkan bahwa instrumen penelitian memiliki tingkat reliabilitas yang semakin baik.

4 Hasil dan Pembahasan

4.1 Hasil Uji Validitas

Pada tahap awal distribusi kuesioner, 20 set data dikumpulkan untuk pengujian validitas dan reliabilitas. Pengujian dilakukan menggunakan koefisien korelasi Pearson untuk setiap dimensi dari 45 butir kuesioner. Dalam 20 responden dan tingkat signifikansi 5%, nilai *r-table* adalah 0,444. Hasil pengujian untuk dimensi pengetahuan dapat dilihat pada Tabel 3. Hasil menunjukkan bahwa setiap butir kuesioner memiliki *r-value* lebih besar dari 0,444 yang menunjukkan bahwa setiap butir instrumen yang digunakan untuk dimensi pengetahuan adalah valid. Analisis serupa juga dilakukan untuk mengetahui validitas instrumen pada dimensi sikap dan perilaku.

Tabel 3 Hasil uji validitas dimensi pengetahuan

Dimensi Pengetahuan			
Fokus Area	**Kuesioner**	**Koefisien Korelasi Pearson (*r-value*)**	**Status**
PM	KPM1	0,808	Valid
	KPM2	0,808	Valid
	KPM3	0,602	Valid
EU	KEU1	0,782	Valid
	KEU2	0,881	Valid
IU	KIU1	0,808	Valid
	KIU2	0,899	Valid
SMU	KSMU1	0,866	Valid
	KSMU2	0,635	Valid
MDU	KMDU1	0,578	Valid
	KMDU2	0,801	Valid
IH	KIH1	0,886	Valid
	KIH2	0,844	Valid
IR	KIR1	0,757	Valid
	KIR2	0,564	Valid

Tabel 4 menunjukkan hasil pengujian validitas untuk dimensi sikap. Hasil menunjukkan bahwa setiap butir kuesioner memiliki *r-value* lebih besar dari 0,444 yang mengindikasikan bahwa instrumen yang digunakan untuk dimensi sikap adalah valid.

 ISSN:2302-8149
e-ISSN:2540-9719

Tabel 4 Hasi uji validitas dimensi sikap

Dimensi Sikap			
Fokus Area	**Kuesioner**	**Koefisien Korelasi Pearson (*r-value*)**	**Status**
PM	APM1	0,878	Valid
	APM2	0,878	Valid
	APM3	0,792	Valid
EU	AEU1	0,843	Valid
	AEU2	0,864	Valid
IU	AIU1	0,878	Valid
	AIU2	0,823	Valid
SMU	ASMU1	0,762	Valid
	ASMU2	0,762	Valid
MDU	AMDU1	0,698	Valid
	AMDU2	0,936	Valid
IH	AIH1	0,792	Valid
	AIH2	0,878	Valid
IR	AIR1	0,720	Valid
	AIR2	0,452	Valid

Tabel 5 menjelaskan hasil uji validitas untuk dimensi perilaku. Hasil uji menunjukkan bahwa semua butir kuesioner memiliki *r-value* lebih besar dari 0,444, yang menegaskan bahwa setiap butir instrumen penelitian adalah valid. Berdasarkan uji validitas untuk semua dimensi, semua butir kuesioner memenuhi kriteria validitas. Oleh karena itu, instrumen yang digunakan untuk mengukur pengetahuan, sikap, dan perilaku dalam penelitian ini dianggap valid dan sesuai untuk digunakan pada tahap penelitian selanjutnya.

Tabel 5 Hasil uji validitas dimensi perilaku

Dimensi Perilaku			
Fokus Area	**Kuesioner**	**Koefisien Korelasi Pearson (r-value)**	**Status**
PM	BPM1	0,539	Valid
	BPM2	0,479	Valid
	BPM3	0,611	Valid
EU	BEU1	0,539	Valid
	BEU2	0,614	Valid
IU	BIU1	0,730	Valid
	BIU2	0,827	Valid
SMU	BSMU1	0,876	Valid
	BSMU2	0,621	Valid
MDU	BMDU1	0,604	Valid
	BMDU2	0,778	Valid
IH	BIH1	0,675	Valid
	BIH2	0,691	Valid
IR	BIR1	0,817	Valid
	BIR2	0,518	Valid

Keterangan
PM : *Password Management*
EU : *Email Use*
IU : *Internet Use*
SMU : *Social Media Use*
MDU : *Mobile Device Use*
IH : *Information Handling*
IR : *Incident Reporting*

 ISSN:2302-8149
e-ISSN:2540-9719

4.2 Hasil Uji Reliabilitas

Hasil pengujian reliabilitas ditunjukkan pada Tabel 6. Dari pengujian yang dilakukan ditemukan bahwa koefisien Cronbach's Alpha untuk masing-masing dimensi adalah lebih besar dari 0,700, dengan demikian instrumen penelitian dikonfirmasi reliabel, sehingga dapat dilanjutkan untuk tahap selanjutnya.

Tabel 6 Hasil uji reliabilitas

Dimensi	Koefisien Cronbach's Alpha
Pengetahuan	0,930
Sikap	0,933
Perilaku	0,883

4.3 Hasil Pengukuran Kesadaran Keamanan Informasi

Berdasarkan hasil kuesioner yang berhasil dikumpulkan, setelah diolah ditemukan hasil seperti yang dijelaskan pada Tabel 7.

Table 7 Hasil pengukuran kesadaran keamanan informasi

Fokus Area	Dimensi K 30%	A 20%	B 50%	Total
Password Management	93,14%	92,84%	87,55%	90,28%
Email Use	93,38%	92,50%	92,06%	92,54%
Internet Use	94,85%	93,09%	92,94%	93,54%
Social Media Use	92,06%	91,03%	91,62%	91,63%
Mobile Device Use	91,03%	90,59%	89,12%	89,99%
Information Handling	91,03%	91,76%	90,88%	91,10%
Incident Reporting	89,41%	90,74%	90,15%	90,04%
Total	92,20%	91,86%	90,41%	91,24%

Hasil tersebut mengonfirmasi bahwa HAIS-Q dapat diterapkan untuk pengukuran tingkat kesadaran keamanan informasi. Berdasarkan hasil tersebut, hasil keseluruhan untuk setiap dimensi dan fokus area berada pada tingkat yang memuaskan yang menunjukkan tidak diperlukan tindakan mendesak untuk perbaikan. Berdasarkan hasil penilaian Kesadaran Keamanan Informasi, skor akhir kesadaran pegawai Pusinfowas tergolong tinggi dengan mencapai nilai 91,24%. Temuan ini mengonfirmasi bahwa pegawai mempraktikkan prinsip keamanan informasi umum, memiliki pemahaman yang kuat tentang keamanan informasi, dan membangun sikap dan perilaku yang baik di tempat kerja terhadap keamanan informasi. Temuan ini sesuai dengan fakta bahwa sebagian besar pegawai Pusinfowas memiliki latar belakang pendidikan terkait TI, yang memberi mereka tingkat literasi TI yang lebih tinggi dan pemahaman yang lebih kuat tentang kesadaran keamanan informasi. Dari hasil persentase dimensi di mana pengetahuan (92,20%), sikap (91,86%), dan perilaku (90,41%), dapat dilihat bahwa pegawai memiliki skor yang lebih rendah pada dimensi perilaku dibanding dua dimensi lainnya. Pola ini juga ditemukan dalam studi keamanan informasi lainnya[17],[18],[19], di mana orang cenderung memiliki pengetahuan yang memadai dan sikap yang baik, namun mereka menghadapi kesulitan yang lebih besar dalam mempraktikkannya ke dalam budaya perilaku yang aman.

Fokus area Penggunaan Internet (*Internet Use*) mencapai skor total tertinggi sebesar 93,54% dibandingkan dengan area fokus lainnya, dengan skor untuk setiap dimensi pengetahuan, sikap, dan perilaku masing-masing sebesar 94,85%, 93,09%, dan 92,94%. Temuan ini selaras dengan penelitian yang dilakukan oleh Prakasan dan Setiawan [20]. Hal ini menunjukkan bahwa pegawai menyadari pentingnya beraktivitas secara aman menggunakan internet untuk pekerjaan atau saat menggunakannya untuk tujuan lain. Hal ini mengindikasikan keberhasilan dari berbagai upaya yang diambil Pusinfowas untuk meningkatkan kesadaran pegawai, seperti pemberitahuan yang konsisten kepada setiap individu.

 ISSN:2302-8149
e-ISSN:2540-9719

Fokus area Penggunaan Email (*Email Use*) menempati peringkat kedua dengan skor tertinggi, dengan total skor 92,54%. Skor untuk setiap dimensi pada fokus area ini juga cukup seimbang. Skor untuk pengetahuan, sikap, dan perilaku masing-masing sebesar 93,38%, 92,50%, dan 92,06%. Temuan ini menunjukkan bahwa responden memiliki pemahaman yang cukup tentang berbagai ancaman keamanan dalam penggunaan email, seperti pesan yang mencurigakan dan lampiran atau tautan berbahaya. Selain itu, penelitian ini menemukan bahwa fokus area Manajemen Kata Sandi (*Password Management*), Penggunaan Media Sosial (*Social Media Use*), Penanganan Informasi (*Information Handling*), dan Pelaporan Insiden (*Incident Reporting*) memiliki skor serupa yakni lebih besar dari 90%, yaitu masing-masing 90,28%, 91,63%, 91,10%, dan 90,04%. Temuan ini menunjukkan bahwa karyawan memiliki pemahaman yang baik tentang manajemen kata sandi, kebijakan media sosial, dan manajemen data dan informasi sensitif, serta secara aktif melaporkan setiap penyimpangan kepada tim dukungan pengguna dan penanganan insiden siber di tempat kerja.

Terakhir, hasil pengukuran menunjukkan bahwa fokus area Penggunaan Perangkat Seluler (*Mobile Device Use*) adalah fokus area dengan skor terendah, dengan total skor 89,99. Hasil dari setiap dimensi juga menunjukkan bahwa skor fokus area penggunaan perangkat seluler adalah yang terendah dibandingkan dengan fokus area lainnya. Temuan ini serupa dengan apa yang telah ditemukan dalam penelitian sebelumnya [21]. Temuan ini menyiratkan bahwa perilaku keamanan menimbulkan banyak tantangan dalam penggunaan perangkat seluler. Meski demikian, dalam penelitian ini skor yang dihasilkan masih berada pada tingkat yang baik, atau kategori aman.

4.4 Rekomendasi

Berdasarkan hasil pengukuran kesadaran keamanan informasi, beberapa rekomendasi diajukan untuk memperkuat tingkat kesadaran keamanan informasi saat ini. Rekomendasi ini secara khusus membahas kesenjangan yang diamati antara pengetahuan, sikap, dan perilaku, serta memperkuat fokus area dengan perbedaan skor yang signifikan dibandingkan dengan fokus area lainnya.

Pertama, organisasi perlu mendorong perilaku yang aman, karena dimensi perilaku secara konsisten menunjukkan skor yang sedikit lebih rendah dibandingkan dengan dimensi pengetahuan dan sikap. Pelatihan berorientasi praktik seperti simulasi dan latihan berbasis skenario dapat membantu pegawai untuk menerapkan pemahaman mereka tentang keamanan informasi ke dalam perilaku yang aman. Pendekatan ini perlu dilakukan secara berkesinambungan untuk memastikan bahwa kesadaran keamanan tidak hanya bersifat teoritis tetapi juga operasional.

Kedua, organisasi harus melakukan intervensi untuk manajemen kata sandi karena memiliki skor perilaku yang lebih rendah dan berada di tiga terbawah untuk total skor. Organisasi disarankan untuk memperkuat mekanisme dukungan teknis pada manajemen kata sandi dan kebijakan kata sandi. Selain itu, organisasi perlu menjadwalkan pengingat berkala dan memperbarui kebijakan untuk memastikan kesesuaian dengan kebijakan yang lebih tinggi berkaitan praktik kata sandi yang aman.

Ketiga, karena skor terendah dari fokus area adalah perangkat seluler, maka dari itu organisasi disarankan untuk mempertimbangkan mengadopsi praktik manajemen perangkat seluler guna mengatasi masalah keamanan dalam lingkup kebocoran data setiap kali perangkat disalahgunakan atau hilang. Selain itu, karyawan perlu diedukasi dalam memisahkan serta menjaga data pribadi dan data pekerjaan. Terakhir, manajemen harus berkomitmen untuk mendorong semua pegawai agar mematuhi peraturan dan strategi yang ada untuk membangun perilaku yang aman di lingkungan pekerjaan.

5 Kesimpulan

Penelitian yang dilakukan berhasil menunjukkan tingkat kesadaran keamanan informasi pegawai di unit kerja Pusat Informasi Pengawasan (Pusinfowas) BPKP. Hasil pengkuran menunjukkan bahwa semua dimensi dan fokus area dalam model HAIS-Q berkinerja pada tingkat yang memuaskan, yaitu kategori “Baik” dengan total skor 91,24%. Hasil tersebut, mengonfirmasi bahwa tidak diperlukan tindakan lebih lanjut yang sifatnya mendesak dalam peningkatan kesadaran keamanan informasi di unit kerja Pusinfowas BPKP. Meski demikian, penelitian ini memberikan beberapa rekomendasi guna memperkuat skor kesadaran keamanan informasi dan membuatnya tetap bertahan pada level “Baik”. Berdasarkan hasil studi ini pegawai Pusinfowas BPKP layak dijadikan sebagai *role model* kesadaran keamanan informasi terhadap pegawai dari unit kerja lain di lingkungan kerja BPKP.

 ISSN:2302-8149
e-ISSN:2540-9719

Penelitian ini terbatas pada pengukuran tingkat kesadaran keamanan informasi di unit kerja Pusinfowas BPKP. Penelitian selanjutnya dapat memperluas cakupan penelitian untuk tingkat organisasi BPKP secara keseluruhan. Selain itu, dari hasil tingkat kesadaran keamanan informasi yang ditemukan, menarik untuk dilakukan analisis lebih lanjut berkaitan faktor-faktor yang mempengaruhi pegawai Pusinfowas memiliki level kesadaran "Baik" sesuai model HAIS-Q.

Referensi

[1] R. Trimanadi and D. I. Sensuse, "*Constraints Assessment in Implementation of Indonesian Government Enterprise Architecture: A Review*," in *2024 International Conference on Smart Computing, IoT and Machine Learning, SIML 2024*, Institute of Electrical and Electronics Engineers Inc., 2024, pp. 145–149. DOI: 10.1109/SIML61815.2024.10578101.

[2] T. Alharbi, "*A Holistic Evaluation Model for Information Security Awareness Programs in Work Environment*," in *Proceedings of the 2023 8th International Conference on Mobile and Secure Services, MobiSecServ 2023*, Institute of Electrical and Electronics Engineers Inc., 2023. DOI: 10.1109/MobiSecServ58080.2023.10329041.

[3] Badan Siber dan Sandi Negara, "Lanskap Keamanan Siber Indonesia 2024," Jakarta, 2024.

[4] Pusat Informasi Pengawasan, "Laporan Kinerja Triwulan 1 2025," Jakarta, 2025.

[5] R. Bisma, M. H. Negara, A. W. Purwita, B. Sisephaputra, and D. F. Suyatno, "*Measurement of Information Security Awareness Level on using Free Wi-Fi in Coffee Shop*," in *2024 7th International Conference on Vocational Education and Electrical Engineering: Charting the Course of Artificial Technology in Sustainable Society, ICVEE 2024*, Institute of Electrical and Electronics Engineers Inc., 2024, pp. 12–18. DOI: 10.1109/ICVEE63912.2024.10823691.

[6] H. Chen, Y. Zhang, S. Zhang, and T. Lyu, "*Exploring the Role of Gamified Information Security Education Systems on Information Security Awareness and Protection Behavioral Intention*," *Educ. Inf. Technol. (Dordr).*, Vol. 28, No. 12, pp. 15915–15948, Dec. 2023, DOI: 10.1007/s10639-023-11771-z.

[7] A. Kavak, "*Impact of Information Security Awareness on Information Security Compliance of Academic Library Staff in Türkiye*," ., Vol. 50, No. 5, Sep. 2024, DOI: 10.1016/j.acalib.2024.102937.

[8] R. Rohan, D. Pal, J. Hautamäki, S. Funilkul, W. Chutimaskul, and H. Thapliyal, "*A Systematic Literature Review of Cybersecurity Scales Assessing Information Security Awareness*," *Heliyon*, Vol. 9, No. 3, Mar. 2023, DOI: 10.1016/j.heliyon.2023.e14234.

[9] Rosihan and A. N. Hidayanto, "*Measurement of Employee Information Security Awareness: A Case Study at an Indonesian Correctional Institution*," in *2022 1st International Conference on Information System and Information Technology, ICISIT 2022*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 318–323. DOI: 10.1109/ICISIT54091.2022.9872988.

[10] V. A. Effendy, Y. Ruldeviyani, M. M. Rifa'i, V. A. Rahmatika, W. Nur'aini, and Y. P. Sagala, "*Measurement of Employee Information Security Awareness on Data Security: A Case Study at XYZ Polytechnic*," in *2022 1st International Conference on Information System and Information Technology, ICISIT 2022*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 272–276. DOI: 10.1109/ICISIT54091.2022.9873077.

[11] F. N. Shakti and A. N. Hidayanto, "*Measurement of Employee Information Security Awareness: Case Study At Financial Institution*," *JITK (Jurnal Ilmu Pengetahuan dan Teknologi Komputer)*, Vol. 9, No. 2, pp. 172–179, Feb. 2024, DOI: 10.33480/jitk.v9i2.4163.

[12] E. Kritzinger, A. Da Veiga, and W. van Staden, "*Measuring Organizational Information Security Awareness in South Africa*," *Information Security Journal*, Vol. 32, No. 2, pp. 120–133, 2023, DOI: 10.1080/19393555.2022.2077265.

[13] N. S. D. Atlanta, C. Candiwan, P. K. Sari, and O. O. Sharif, "*Information Security Awareness Evaluation of Telemedicine Application Users using Human Aspect Information System Questionnaire*," in *2022 IEEE 8th International Conference on Computing, Engineering and Design, ICCED 2022*, Institute of Electrical and Electronics Engineers Inc., 2022. DOI: 10.1109/ICCED56140.2022.10010445.

[14] F. Nyimbili and L. Nyimbili, "*Types of Purposive Sampling Techniques with Their Examples and Application in Qualitative Research Studies*," *British Journal of Multidisciplinary and Advanced Studies*, Vol. 5, No. 1, pp. 90–99, Feb. 2024, DOI: 10.37745/bjmas.2022.0419.

[15] J. Zhen, K. Dong, Z. Xie, and L. Chen, "*Factors Influencing Employees' Information Security Awareness in the Telework Environment*," *Electronics (Switzerland)*, Vol. 11, No. 21, Nov. 2022, DOI: 10.3390/electronics11213458.

[16] S. C. Izah, L. Sylva, and M. Hait, "*Cronbach's Alpha: A Cornerstone in Ensuring Reliability and Validity in Environmental Health Assessment*," Mar. 01, 2024, *Engineered Science Publisher*. DOI: 10.30919/esee1057.

[17] M. A. Rasyidin, A. Putri, M. D. Lestari, R. Nurnajmah, and D. A. Safaraz, "Analisis Kesadaran Mahasiswa dalam Menjaga Keamanan Data Pribadi pada Penggunaan Media," *Jurnal Teknik Informatika dan Teknologi Informasi*, Vol. 5, No. 3, pp. 752–761, Dec. 2025, DOI: 10.55606/jutiti.v5i3.6583.

[18] N. Gede, P. S. Ananda, G. Arna, J. Saskara, B. Gede, and K. Yudistira, "Analisis Kesadaran Keamanan Informasi Penggunaan Layanan *M-Banking* menggunakan *Human Aspects of Information Security Questionnaire*," 2025. [Online]. Available: https://djournals.com/jieee

[19] T. Ramadhan and B. Purwandari, "Analisis Tingkat Kesadaran Keamanan Informasi: Studi Kasus Pengguna Aplikasi Perbankan Digital di Indonesia Guna Mencegah *Social Engineering*," *Syntax Idea*, Vol. 5, p. 86, Jan. 2023, DOI: 10.36418/syntax-idea.v5i1.2113.

[20] D. A. Perkasa and B. Setiawan, "*Measuring Information Security Awareness Level of High School Students*," *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, Vol. 4, No. 4, pp. 1301–1308, Jul. 2024, DOI: 10.57152/malcom.v4i4.1461.