The Indonesian Journal of Computer Science
www.ijcs.net
Volume 13, Issue 6, December 2024
https://doi.org/10.33022/ijcs.v13i6.4536

Eksplorasi Kesadaran dan Faktor Budaya Keamanan Terhadap Keamanan Informasi Dinas Komunikasi dan Informatika Kabupaten XYZ

Michael Parlindungan[1], Setiadi Yazid[2]
michael.parlindungan@ui.ac.id[1], setiadi@cs.ui.ac.id[2]
[1,2] Universitas Indonesia

Informasi Artikel

Diterima : 10 Des 2024
Direvisi : 19 Des 2024
Disetujui : 30 Des 2024

Kata Kunci

Kesadaran Keamanan Informasi, HAIS-Q, KAB, Budaya Keamanan Informasi

Abstrak

Peran teknologi informasi dalam sektor pemerintahan bertujuan menyelenggarakan sistem pemerintahan elektronik yang efisien, akuntabel, dan transparan. Aspek manusia menjadi aspek yang terlemah dan memegang peranan terpenting dalam menjaga keamanan informasi. Dinas Kominfo Kabupaten XYZ memegang peran penting dalam penyelenggaraan pemerintahan daerah, termasuk manajemen sistem informasi dan pengamanan informasi. Penelitian ini mengukur tingkat kesadaran keamanan informasi terhadap 86 pegawai di Dinas Kominfo Kabupaten XYZ menggunakan kuesioner berdasarkan metode HAIS-Q dan aspek budaya keamanan informasi. Hasil penelitian menunjukkan tingkat kesadaran keamanan pegawai berada dalam kategori "cukup". Area manajemen kata sandi, penggunaan *email* dan internet menunjukkan tingkat kesadaran yang "buruk", dan penggunaan media sosial, perangkat *mobile*, penanganan informasi, dan pelaporan insiden berada pada kategori "cukup". Aspek budaya keamanan juga memengaruhi tingkat kesadaran keamanan pegawai dimana berada pada kategori "cukup". Berdasarkan hasil tersebut, rekomdendasi peningkatan kesadaran diperlukan, seperti pembuatan kebijakan dan pedoman keamanan informasi, serta pelaksanaan program kesadaran keamanan informasi.

Keywords

Information Security Awareness, HAIS-Q, KAB, Information Security Culture

Abstract

The role of information technology in the government sector is to organize an efficient, accountable, and transparent electronic government system. The human aspect is the weakest and plays the most important role in maintaining information security. The XYZ District and Communication Agency is important in organizing regional government, including information system management and information security. This study measured the level of information security awareness of 86 employees at the XYZ District Kominfo Agency using a questionnaire based on the HAIS-Q method and aspects of information security culture. The results showed that the level of employee security awareness was at the "average" level. The areas of password management, email, and internet use showed a "poor" level of awareness, and the use of social media, mobile devices, information handling, and incident reporting was at the "average" level. The security culture aspect also influenced the level of employee security awareness which was at the "average" level. Based on the results, recommendations for increasing awareness are needed, such as the creation of information security policies and guidelines, and the implementation of information security awareness programs.

A. Pendahuluan

Penggunaan teknologi informasi pada sektor pemerintahan dilakukan dengan penyelenggaraan sistem pemerintahan secara elektronik dengan menggunakan Sistem Pemerintahan Berbasis Elektronik (SPBE) [1]. Tujuannya adalah untuk menyelenggarakan sistem pemerintahan elektronik yang efisien, transparan, dan akuntabel secara nasional, baik di pemerintah pusat maupun di pemerintah daerah.

Dengan perkembangan penggunaan teknologi informasi di pemerintahan daerah tersebut, pemerintah daerah harus waspada terhadap adanya ancaman keamanan informasi yang semakin meningkat. Menurut data yang dikeluarkan oleh BSSN pada tahun 2023, ditemukan sebanyak 347 dugaan insiden keamanan informasi di Indonesia, dengan 186 kasus di antaranya terjadi pada administrasi pemerintahan [2]. Insiden tersebut terdiri dari kebocoran data, *ransomware, web defacement*, pemantauan dugaan insiden, dan potensi serangan *DdoS*.

Hal yang sama juga ditunjukkan dengan layanan Gov-CSIRT Indonesia yang telah menangani sebanyak 229 kasus insiden keamanan informasi pada sektor pemerintahan [3]. Berdasarkan hal tersebut, potensi ancaman keamanan informasi diprediksi akan terus meningkat setiap tahunnya. Hal ini menunjukkan keamanan informasi sangat vital di tengah semakin banyaknya ancaman insiden keamanan yang terjadi untuk melindungi ketersediaan, kerahasiaan, dan integritas informasi dan aset yang dimiliki [4], [5]

Aspek manusia, proses, dan teknologi menjadi kombinasi yang efektif untuk melindungi organisasi dari ancaman insiden keamanan [6]. Dimana aspek manusia merupakan aspek yang paling lemah dan menjadi bagian yang paling penting dalam menjaga keamanan informasi [7]. Upaya mengurangi risiko dan menjaga keamanan informasi dalam aspek manusia di organisasi dapat dilakukan dengan memperbarui kebijakan keamanan, melakukan edukasi kepada pegawai, hingga memantau aktivitas pegawai [8]. Pengukuran kesadaran keamanan menjadi kerangka awal untuk program edukasi kesadaran keamanan [9]. Penelitian yang dilakukan Parsons et al. [10] mengukur kesadaran keamanan informasi pada pegawai menggunakan metode HAIS-Q. Selanjutnya, metode ini telah dipakai untuk mengukur tingkat kesadaran keamanan pegawai di berbagai organisasi, termasuk di instansi pemerintahan [11], [12]. Kemudian, penelitian yang dilakukan Wiley et al. [13] meneliti pengaruh budaya keamanan terhadap tingkat kesadaran keamanan pegawai.

Dinas Komunikasi dan Informatika Kabupaten XYZ memiliki peran strategis dalam membantu penyelenggaraan pemerintahan daerah, termasuk manajemen sistem informasi dan pengamanan informasi yang berfokus pada kerahasiaan, konsistensi, dan ketersediaan. Hal ini memengaruhi kualitas penyelenggaraan pemerintah daerah dan pelayanan masyarakat yang responsif dan akuntabel. Berdasarkan hal tersebut, kesadaran keamanan informasi sangat penting bagi pegawai Dinas Kominfo Kabupaten XYZ untuk dapat menjalankan tugasnya dengan baik.

Oleh karena itu, penelitian ini bertujuan untuk mengukur tingkat kesadaran pegawai Dinas Kominfo Kabupaten XYZ terhadap keamanan informasi. penelitian ini menggunakan metode HAIS-Q dan aspek budaya keamanan untuk melihat pengaruh budaya keamanan terhadap tingkat kesadaran keamanan informasi.

Hingga saat ini belum pernah dilakukan pengukuran tingkat kesadaran pegawai Dinas Kominfo Kabupaten XYZ terhadap keamanan informasi.

Sistematis dalam penulisan penelitian ini terdiri dari latar belakang penelitian, tinjauan literatur berdasarkan teori-teori dan penelitian terdahulu, metode penelitian menjelaskan instrumen yang digunakan dalam penelitian, hasil dan pembahasan dari penelitian yang dilakukan, serta rekomendasi dan simpulan penelitian.

B. Tinjauan Literatur

1. Kesadaran Keamanan Informasi

Pemahaman kesadaran keamanan informasi terdiri atas dua aspek [14], dimana aspek pertama terkait sejauh mana pemahaman pegawai terhadap perilaku keamanan informasi yang aman, dan aspek kedua berfokus pada tingkat komitmen dan perilaku pegawai sesuai dengan *best practices* sesuai dengan kebijakan, aturan dan pedoman keamanan informasi.

Kesadaran keamanan informasi merupakan kerangka awal penting dari pembelajaran keamanan informasi yang berkesinambungan [15]. Meningkatkan tingkat kesadaran keamanan informasi menjadi cara yang yang efektif dalam menjaga keamanan informasi di perusahaan atau instansi [16]. Hal tersebut tidak terlepas dari faktor manusia yang menjadi aspek yang terlemah dalam rantai kesadaran keamanan informasi [17]. Kesadaran keamanan informasi menjadi kebutuhan yang penting dalam memenuhi *best practices* dan menjadi bagian yang mendasar dari manajemen keamanan informasi yang efektif.

2. Model *Knowledge, Attitude, Behavior* (KAB)

Model *knowledge*, *attitude*, dan *behaviour* (KAB) [18] merupakan salah satu model yang diadopsi untuk mengukur kesadaran keamanan informasi. Model ini terdiri dari tiga aspek, yaitu aspek *knowledge* yaitu pengetahuan terhadap keamanan informasi, aspek *attitude* berkaitan dengan sikap terhadap keamanan informasi, dan aspek *behaviour* berkaitan dengan perilaku keamanan informasi. Model ini menggunakan komponen model psikologis sosial yang saling berkaitan [19], [20]. Model KAB menggunakan skala pengukuran tingkat kesadaran keamanan yang dapat dilihat pada tabel 1 berikut.

Tabel 1. Skala Pengukuran Kesadaran Keamanan Informasi

Tingkat Kesadaran	Ukuran (%)
Baik	80-100
Cukup	60-79
Buruk	≤59

Ketiga aspek dalam model KAB saling berkaitan, dimana pengetahuan seseorang terhadap kebijakan dan prosedur keamanan informasi berpengaruh terhadap perubahan sikap terhadap keamanan informasi dan menghasilkan perilaku keamanan informasi [21], [22], [23].

3. *Human Aspects of Information Security Questionnaire* (HAIS-Q)

Metode HAIS-Q merupakan pengembangan dari model KAB untuk mengukur tingkat kesadaran keamanan informasi [14]. Alat metode ini terdiri dari 63 item

untuk mengukur tujuh area fokus, yaitu manajemen kata sandi, penggunaan *email*, penggunaan internet, penggunaan media sosial, perangkat seluler, penanganan informasi, dan pelaporan insiden. Setiap area fokus tersebut terdiri dari tiga sub-area fokus sehingga terdapat 21 sub-area fokus yang diukur berdasarkan aspek pada model KAB yaitu aspek pengetahuan, sikap, dan perilaku.

4. Budaya Keamanan Informasi

Budaya keamanan mencakup sikap, asumsi, nilai, keyakinan, dan pengetahuan dari pegawai untuk berinteraksi dengan sistem organisasi dan melakukan prosedur, tugas, dan aktivitas pekerjaan sehari-hari yang relevan [13]. Budaya keamanan yang kuat dapat terjadi jika pegawai menyadari risiko keamanan dan tindakan pencegahan, serta tanggung jawab pegawai dan langkah-langkah yang diambil untuk meningkatkan keamanan informasi. Hal tersebut bertujuan untuk melindungi aset informasi dari organisasi dengan menciptakan lingkungan kerja yang mendukung pegawai dalam perilaku keamanan yang benar [13]. Aspek budaya keamanan pada penelitian ini terdiri dari pengetahuan dan tanggung jawab tentang keamanan informasi, pengetahuan insiden keamanan, program kesadaran keamanan, evaluasi kepatuhan, dan persyaratan (*requirements*) keamanan informasi.

5. Penelitian Sebelumnya

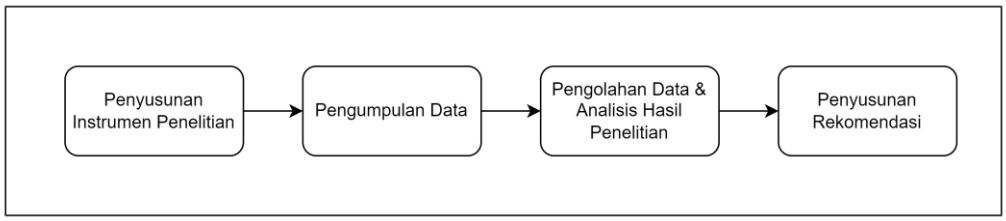
Beberapa penelitian sebelumnya telah menjelaskan penggunaan metode HAIS-Q untuk mengukur kesadaran keamanan informasi pegawai di lingkungan kerja. Penelitian yang dilakukan Mahardika et al. [12] mengukur tingkat kesadaran keamanan informasi pada pegawai Pusat Analisis dan Layanan Informasi Komisi Yudisial. Penelitian ini menggunakan HAIS-Q dan dilakukan dengan menyebarkan kuesioner kepada 25 responden pegawai Palinfo dan wawancara tambahan kepada pegawai pada unit Data dan TI. Hasilnya menunjukkan tingkat kesadaran keamanan informasi pegawai sebesar 78,10 yang berada pada tingkat cukup.

Effendy et al. [24] melakukan penelitian untuk mengukur tingkat kesadaran keamanan informasi pegawai di Politeknik XYZ. Penelitian ini menggunakan HAIS-Q dan diolah menggunakan metode *Analytical Hierarchy Process* (AHP). Pengumpulan data dilakukan kepada 53 responden pegawai instansi tersebut.

Wiley et al. [13] melakukan penelitian untuk mengeksplorasi hubungan antara kesadaran keamanan informasi, budaya organisasi, dan budaya keamanan. Penelitian ini dilakukan kepada pekerja di Australia dengan menggunakan HAIS-Q dan digabungkan dengan *Denison Organizational Culture Survey* (DOCS) untuk mengukur budaya organisasi serta *Organizational Security Culture Measure* (OSCM) untuk mengukur budaya keamanan informasi. Hasil penelitian menunjukkan terdapat hubungan positif antara budaya keamanan, budaya organisasi, dan kesadaran keamanan informasi.

C. Metode Penelitian

Tahapan dalam penelitian ini terdiri dari menyusun instrumen penelitian, pengumpulan data, pengolahan data dan analisis hasil penelitian, serta menyusun rekomendasi yang dapat dilihat pada Gambar 1 berikut.



Gambar 1. Tahapan Penelitian

1. Penyusunan Instrumen Penelitian

Penelitian ini menggunakan metode instrumen HAIS-Q [14] berdasarkan aspek pengetahuan, sikap, dan perilaku pada model KAB [18]. Metode HAIS-Q berfokus pada tujuh area fokus yang terdiri dari manajemen kata sandi, penggunaan *email*, penggunaan internet, penggunaan media sosial, perangkat *mobile*, penanganan informasi, dan pelaporan insiden. Kemudian dilakukan penyesuaian pada instrumen kuesioner dengan menambahkan area fokus budaya keamanan informasi seperti yang dijelaskan oleh Wiley et al (2020) [13]. Pada metode HAIS-Q memiliki total 63 pernyataan, dimana masing-masing aspek pengetahuan, sikap, dan perilaku terdiri dari 21 pernyataan dengan setiap area fokus terdiri dari 3 pernyataan. Area fokus budaya keamanan informasi terdiri dari 6 pernyataan. Sehingga, keseluruhan item pernyataan berjumlah sebanyak 69 item pernyataan. Selanjutnya, instrumen kuesioner dilakukan validasi oleh ahli dan uji keterbacaan kepada beberapa responden pegawai Dinas Kominfo Kabupaten XYZ melalui diskusi dan wawancara. Tabel 2 menunjukkan instrumen kuesioner model pengukuran yang telah dilakukan penyesuaian berdasarkan kebutuhan organisasi.

Tabel 2. Instrumen Kuesioner

Aspek/Area Fokus		Sub-Area
Manajemen Kata Sandi	1	Menggunakan kata sandi yang sama
	2	Membagikan kata sandi
	3	Memilih kata sandi yang kuat
Penggunaan *Email*	1	Membuka *link* pada *email* dari pengirim yang dikenal
	2	Membuka *link* pada *email* dari pengirim tidak dikenal
	3	Membuka *attachment* dari pengirim tidak dikenal
Penggunaan Internet	1	*Download* file ke perangkat kerja
	2	Mengakses situs tidak berkaitan dengan pekerjaan
	3	Memasukkan informasi pada *website* yang membantu pekerjaan
Penggunaan Media Sosial	1	Memeriksa pengaturan privasi media sosial
	2	Konsekuensi memposting di media sosial
	3	Memposting terkait pekerjaan di media sosial
Perangkat *Mobile*	1	Mengamankan perangkat kerja ketika bekerja di tempat publik
	2	Mengirim file pekerjaan lewat jaringan *wi-fi* publik

Aspek/Area Fokus		Sub-Area
Penanganan Informasi	3	Mengamankan dokumen sensitif/rahasia di perangkat kerja
	1	Membuang berkas pekerjaan sensitif/rahasia
	2	Mencolok *flashdisk*/USB tidak dikenal di perangkat kerja
	3	Meninggalkan berkas sensitif di meja kerja
Pelaporan Insiden	1	Melaporkan perilaku yang membahayakan keamanan informasi
	2	Mengabaikan perilaku keamanan yang buruk
	3	Mengabaikan insiden keamanan
Budaya Keamanan Informasi	1	Pengetahuan terhadap keamanan informasi
	2	Tanggung jawab terhadap keamanan informasi
	3	Insiden/risiko keamanan informasi
	4	Pelaksanaan program kesadaran keamanan informasi
	5	Pemantauan dan evaluasi kebijakan keamanan informasi
	6	Persyaratan keamanan informasi

2. Pengumpulan Data

Penelitian ini dilakukan di lingkungan Dinas Kominfo Kabupaten XYZ. Proses pengumpulan data telah melalui izin dari Kepala Bidang Persandian Dinas Kominfo Kabupaten XYZ. Pengumpulan data dilakukan menggunakan *Google Form* dan disebarkan kepada sebanyak 87 responden pegawai Dinas Kominfo Kabupaten XYZ. Dari hasil penyebaran kuesioner didapatkan sebanyak 86 responden yang valid dimana terdapat 1 jawaban responden yang homogen sehingga dilakukan eliminasi.

3. Pengolahan Data dan Analisis

Jawaban responden hasil pengumpulan data kuesioner akan diolah untuk mengetahui nilai tingkat kesadaran keamanan informasi pegawai dan dipetakan berdasarkan model KAB pada Tabel 1 sebelumnya. Jawaban responden pada kuesioner menggunakan skala *Likert* 5 poin untuk mengetahui tingkat persetujuan responden terhadap suatu pernyataan [25]. Tabel 3 menunjukkan skala *Likert* yang digunakan pada penelitian ini.

Tabel 3. Skala *Likert* 5 Poin

Skor Jawaban	Jawaban
1	Sangat Tidak Setuju
2	Tidak Setuju
3	Ragu-Ragu
4	Setuju
5	Sangat Setuju

4. Penyusunan Rekomendasi

Setelah melakukan pengolahan data dan analisis hasil penelitian, tahap selanjutnya adalah melakukan penyusunan rekomendasi untuk peningkatan kesadaran keamanan informasi pegawai di Dinas Kominfo Kabupaten XYZ. Penyusunan rekomendasi melibatkan diskusi dan validasi kepada ahli.

D. Hasil dan Pembahasan

1. Demografi Responden Penelitian

Responden kuesioner pada penelitian ini merupakan pegawai Dinas Kominfo Kabupaten XYZ. Kuesioner disebarkan kepada 87 responden, namun dari hasil pemeriksaan jawaban kuesioner menggunakan 86 responden. Demografi responden secara umum dapat dilihat pada Tabel 4 berikut.

Tabel 4. Demografi Responden Penelitian

Variabel Demografi	Item	Persentase
Umur	< 26 Tahun	11,6%
	26-41 Tahun	57%
	42-57 Tahun	31,4%
Jenis Kelamin	Laki-Laki	60,5%
	Perempuan	39,5%
Pendidikan	SLTA/Sederajat	24,4%
	D-I-D-III	1,2%
	D-IV/S1	66,3%
	S2	7%
	S3	1,2%
Lama Bekerja	< 1 Tahun	2,3%
	1-5 Tahun	25,6%
	6-10 Tahun	34,9%
	11-15 tahun	18,6%
	>15 Tahun	18,6%

2. Hasil Uji Validitas dan Reliabilitas

Kuesioner yang telah berhasil dikumpulkan akan dilakukan uji validitas dan reliabilitas. Pengujian validitas dan reliabilitas dilakukan dengan menggunakan alat bantu aplikasi SPSS 27. Uji validitas merupakan tahapan penelitian untuk melihat suatu alat ukur dinyatakan valid [26], [27]. Pada pengujian validitas dilakukan perhitungan menggunakan nilai korelasi *Pearson*, dengan nilai korelasi pada taraf signifikansi 5% yang digunakan adalah 0,212. Nilai korelasi tersebut dipakai berdasarkan jumlah responden kuesioner sebanyak 86 responden. Pengujian validitas dilakukan dengan mengelompokkan item kuesioner berdasarkan mdeol KAB dan budaya keamanan informasi. Hasil uji validitas menunjukkan bahwa semua item kuesioner dinyatakan valid.

Setelah melakukan uji validitas, tahap selanjutnya melakukan uji reliabilitas. Uji reliabilitas digunakan untuk menguji konsistensi atau stabilitas pada alat ukur [26], [27]. Uji reliabilitas dilakukan menggunakan nilai koefisien *Cronbach's Alpha* dengan dasar jika nilai koefisien reliabilitas ≥ 0,70 maka kuesioner dianggap reliabel dan dapat diandalkan. Uji reliabilitas kuesioner dibagi berdasarkan 4 aspek, yaitu model KAB dan aspek budaya keamanan informasi. Hasil uji reliabilitas dapat dilihat pada Tabel 5 berikut.

Tabel 5. Hasil Uji Reliabilitas

Aspek	*Cronbach's Alpha*	Keterangan
Pengetahuan	0,944	Reliabel
Sikap	0,949	Reliabel
Perilaku	0,951	Reliabel
Budaya Keamanan Informasi	0,906	Reliabel

Hasil uji reliabilitas pada Tabel 4 menunjukkan semua item kuesioner dapat dinyatakan reliabel dan dapat diandalkan.

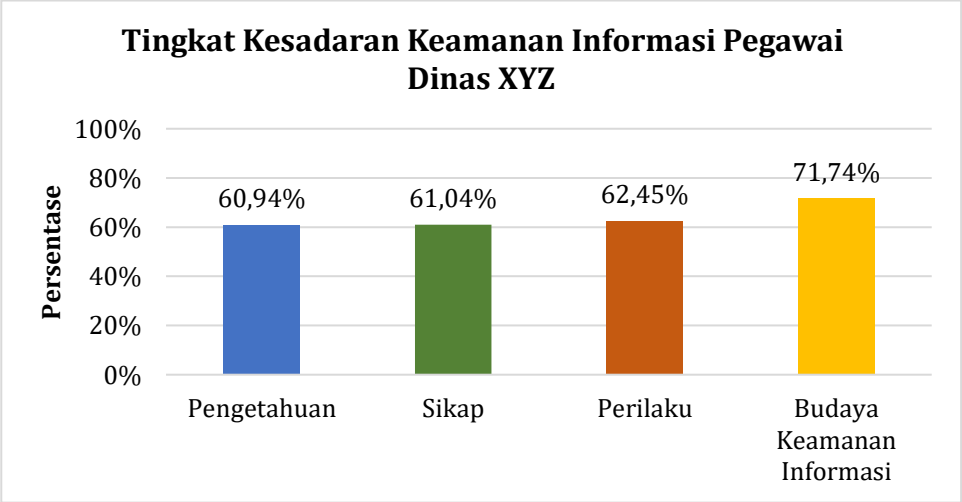
3. Hasil Pengukuran Tingkat Kesadaran Keamanan Informasi

Setelah melakukan uji validitas dan reliabilitas pada jawaban kuesioner, tahap selanjnutnya adalah mengukur tingkat kesadaran keamanan informasi pegawai Dinas Kominfo Kabupaten XYZ dari setiap area fokus berdasarkan model KAB dengan skala pengukuran tingkat kesadaran pada Tabel 1 diatas. Hasil pengukuran tingkat kesadaran keamanan informasi pegawai Dinas Kominfo Kabupaten XYZ dapat dilihat pada Tabel 6 berikut.

Tabel 6. Hasil Pengukuran Tingkat Kesadaran Keamanan Informasi Pegawai Berdasarkan Area Fokus

Area Fokus	Aspek			Tingkat Kesadaran
	Pengetahuan	Sikap	Perilaku	
Manajemen Kata Sandi	52,64%	54,81%	55,81%	**54,42%**
Penggunaan *Email*	53,02%	51,71%	53,57%	**52,77%**
Penggunaan Internet	43,88%	44,96%	44,96%	**44,60%**
Penggunaan Media Sosial	69,77%	72,33%	72,56%	**71,55%**
Perangkat *Mobile*	74,50%	72,33%	74,26%	**73,70%**
Penanganan Informasi	71,71%	71,71%	73,10%	**72,17%**
Pelaporan Insiden	62,09%	59,46%	62,87%	**61,47%**
Tingkat Kesadaran	**60,94%**	**61,04%**	**62,45%**	**61,48%**

Pada aspek budaya keamanan informasi juga diukur menggunakan skala pengukuran tingkat kesadaran pada Tabel 1 diatas dan mendapatkan hasil sebesar 71,74%. Hasil keseluruhan tingkat kesadaran keamanan informasi berdasarkan aspek KAB dan budaya keamanan informasi dapat dilihat pada Gambar 2 berikut.



Gambar 2. Grafik Tingkat Kesadaran Keamanan Informasi

Berdasarkan hasil pada Tabel 2, rata-rata tingkat kesadaran keamanan informasi pegawai Dinas Kominfo Kabupaten XYZ sebesar 61,48% dan berada dalam kategori Cukup. Aspek pengetahuan memperoleh nilai sebesar 60,94%, aspek sikap sebesar 61,04%, dan aspek perilaku sebesar 62,45%. Terdapat 3 area fokus yang berada dalam kategori butuk, yaitu aspek manajemen kata sandi (54,42%), aspek penggunaan *email* (52,77%), dan aspek 44,60%. Hal ini menunjukkan tingkat kesadaran keamanan yang rendah, terutama dalam aspek pengetahuan, yang berpengaruh terhadap sikap dan perilaku pegawai terhadap keamanan informasi. Area fokus lainnya seperti penggunaan media sosial (71,55%), perangkat *mobile* (73,70%), penanganan informasi (72,17%), dan pelaporan insiden (61,47%) berada dalam kategori Cukup. Meskipun pada area fokus pelaporan insiden, aspek sikap pegawai menunjukkan tingkat kesadaran yang buruk dengan memperoleh nilai 59,46%. Berdasarkan hasil diatas, perlu dilakukan upaya untuk dapat meningkatkan kesadaran keamanan informasi pegawai di Dinas Kominfo Kabupaten XYZ.

Hasil pengukuran terhadap budaya keamanan informasi seperti pada Gambar 2 memperoleh nilai 71,74% yang berada pada kategori Cukup. Hasil ini menunjukkan budaya keamanan berpengaruh terhadap tingkat kesadaran keamanan informasi pegawai, seperti yang dijelaskan oleh Wiley et al. [13]. Wiley et al. menjelaskan bahwa semakin baik budaya keamanan informasi di tempat kerja maka memengaruhi tingginya sikap dan perilaku keamanan informasi pegawai. Artinya, budaya keamanan informasi di lingkungan Dinas Kominfo Kabupaten XYZ masih kurang.

Berdasarkan hasil evaluasi tingkat kesadaran pegawai Dinas Kominfo Kabupaten XYZ, perlu dilakukan perbaikan dan peningkatan pada setiap area fokus keamanan informasi. Misalnya, rekomendasi dalam pembuatan kebijakan dan prosedur/pedoman terkait manajemen keamanan informasi yang mengatur setiap area fokus keamanan informasi. Misalnya pada area manajemen kata sandi, perlu dibuat prosedur yang mengatur manajemen kata sandi, seperti penggunaan kata sandi yang berbeda antara akun pribadi dengan akun kerja, penggunaan kata sandi yang aman, dan aturan untuk tidak membagikan kata sandi. Selain itu, perlu

dilakukan integrasi layanan *single sign-on* pada seluruh aplikasi dan sistem di Dinas Kominfo Kabupaten XYZ yang membutuhkan autentikasi. Dalam aspek penggunaan *email* dan internet, diperlukan pembuatan pedoman dan kebijakan terkait penggunaan *email* yang aman dan mengatur akses internet di lingkungan kerja, termasuk dalam hal mengunduh *file* dari internet, pembatasan akses situs tidak resmi dan tidak terkait pekerjaan saat jam kerja, dan memasukkan informasi terkait pekerjaan pada *website* tertentu. Dalam area penggunaan media sosial, perlu dibuat kebijakan terkait penggunaan media sosial di lingkungan kerja, termasuk dalam hal memposting terkait pekerjaan di media sosial. Dalam hal perangkat *mobile* dan penanganan informasi, perlu dibuat kebijakan yang mengatur dalam hal pengguaan perangkat kerja seperti *laptop* di tempat publik, pengiriman berkas pekerjaan dengan menggunakan *virtual private network* (VPN) jika melalui *wi-fi* publik, dan penanganan dokumen penting, termasuk penghancuran dokumen rahasia dan pengurangan penggunaan *removable* media untuk melakukan transfer berkas pekerjaan. Setiap perangkat kerja wajib pula dilindungi oleh *antivirus* dan *firewall.* Pada area pelaporan insiden, perlu dibuat kebijakan yang mengatur kewajiban pelaporan seluruh insiden keamanan informasi kepada tim keamanan (Tim CSIRT) Dinas Kominfo Kabupaten XYZ.

Selain membuat kebijakan dan pedoman/prosedur, perlu dilaksanakan program kesadaran keamanan informasi secara rutin untuk meningkatkan pengetahuan dan sikap pegawai dalam mematuhi keamanan informasi di lingkungan Dinas Kominfo Kabupaten XYZ. Program kesadaran keamanan seperti sosialisasi dan pelatihan formal melalui rapat, seminar dan diskusi, simulasi atau pelatihan seperti *phishing, spam* perlu dilakukan. Selain itu, media sosial Dinas Kominfo Kabupaten XYZ dapat dimanfaatkan untuk menyampaikan pesan dan kampanye keamanan informasi. Terakhir, program kesadaran dapat dibuat dalam bentuk buku pedoman keamanan informasi yang berisi prosedur dan standar keamanan informasi berdasarkan area fokus keamanan yang wajib dipatuhi oleh pegawai Dinas Kominfo Kabupaten XYZ. Penyusunan rekomendasi ini telah didiskusikan dan divalidasi oleh ahli dari Universitas Indonesia.

E. Simpulan

Penelitian pengukuran tingkat kesadaran keamanan informasi pegawai Dinas Kominfo Kabupaten XYZ dilakukan dengan menggunakan kombinasi metode HAIS-Q dan budaya keamanan informasi. Kuesioner penelitian ini memiliki 4 aspek berdasarkan model KAB [18] dan budaya keamanan informasi [13] dan mencakup 7 area fokus keamanan informasi yang telah disesuaikan berdasarkan kondisi organisasi. Penelitian ini menilai pentingnya mengevaluasi tingkat kesadaran keamanan informasi pegawai, dan pentingnya peningkatan kesadaran keamanan informasi berdasarkan rekomendasi yang telah diberikan.

Penelitian ini dapat memberikan gambaran mengenai pengukuran kesadaran keamanan informasi di instansi atau dinas pemerintahan daerah. Penelitian selanjutnya dapat mengombinasikan aspek-aspek lain seperti sanksi (*punishment*) dan penghargaan (*reward*), simulasi keamanan informasi, dan peninjauan terhadap infrastruktur teknologi *existing* yang ada di organisasi, serta menambahkan area fokus keamanan informasi berdasarkan standar ISO/EIC 27001:2022.

F. Ucapan Terima Kasih

Penulis berterima kasih kepada Dinas Kominfo Kabupaten XYZ yang telah memberikan dukungan data terhadap penelitian ini sehingga dapat diselesaikan dengan baik. Penulis juga berterima kasih kepada dosen pembimbing yang telah memberikan dukungan serta saran terhadap penelitian ini.

G. Referensi

[1] Indonesia, "Peraturan Presiden (PERPRES) Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik." p. 110, 2018. [Online]. Available: https://peraturan.bpk.go.id/Details/96913/perpres-no-95-tahun-2018

[2] Badan Siber dan Sandi Negara RI, "Lanskap Keamanan Siber Indonesia 2023," Jakarta, 2024.

[3] Badan Siber dan Sandi Negara RI, "Laporan GOV-CSIRT 2019," Jakarta, 2019. [Online]. Available: https://govcsirt.bssn.go.id/laporan-tahunan-gov-csirt-2019/

[4] S. AlGhamdi, K. T. Win, and E. Vlahu-Gjorgievska, "Information security governance challenges and critical success factors: Systematic review," *Comput. Secur.*, vol. 99, p. 102030, 2020, doi: https://doi.org/10.1016/j.cose.2020.102030.

[5] H. N. Chua, J. S. Teh, and A. Herbland, "Identifying the Effect of Data Breach Publicity on Information Security Awareness Using Hierarchical Regression," *IEEE Access*, vol. 9, pp. 121759–121770, 2021, doi: 10.1109/ACCESS.2021.3107426.

[6] H. F. Tipton and M. Krause, *Information.Security.Management.Handbook.* 2007.

[7] G. Assenza, A. Chittaro, M. C. De Maggio, M. Mastrapasqua, and R. Setola, "A Review of Methods for Evaluating Security Awareness Initiatives," *Eur. J. Secur. Res.*, vol. 5, no. 2, pp. 259–287, 2020, doi: 10.1007/s41125-019-00052-x.

[8] G. Butaka, "Human Error in Cyberspace," ISACA. [Online]. Available: https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2021/volume-38/human-error-in-cyberspace

[9] Y. Normandia, L. Kumaralalita, A. N. Hidayanto, W. S. Nugroho, and M. R. Shihab, "Measurement of employee information security awareness using analytic hierarchy process (AHP): A case study of foreign affairs ministry," *Proc. - 2018 4th Int. Conf. Comput. Eng. Des. ICCED 2018*, pp. 52–56, 2019, doi: 10.1109/ICCED.2018.00020.

[10] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)," *Comput. Secur.*, vol. 42, pp. 165–176, 2014, doi: 10.1016/j.cose.2013.12.003.

[11] Rosihan and A. N. Hidayanto, "Measurement of Employee Information Security Awareness: A Case Study at an Indonesian Correctional Institution," *2022 1st Int. Conf. Inf. Syst. Inf. Technol. ICISIT 2022*, pp. 318–323, 2022, doi: 10.1109/ICISIT54091.2022.9872988.

[12] M. S. Mahardika, A. N. Hidayanto, P. A. Paramartha, L. D. Ompusunggu, R. Mahdalina, and F. Affan, "Measurement of employee awareness levels for

information security at the center of analysis and information services judicial commission Republic of Indonesia," *Adv. Sci. Technol. Eng. Syst.*, vol. 5, no. 3, pp. 501 – 509, 2020, doi: 10.25046/aj050362.

[13] A. Wiley, A. McCormac, and D. Calic, "More than the individual: Examining the relationship between culture and Information Security Awareness," *Comput. Secur.*, vol. 88, p. 101640, 2020, doi: https://doi.org/10.1016/j.cose.2019.101640.

[14] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans, "The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies," *Comput. Secur.*, vol. 66, pp. 40–51, 2017, doi: 10.1016/j.cose.2017.01.004.

[15] P. Bowen, J. Hash, M. Wilson, C. M. Gutierrez, and W. Jeffrey, *Information Security Handbook: A Guide for Managers*, no. October. National Institute of Standards and Technology, 2006. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-100.pdf

[16] A. McIlwraith, *Information Security and Employee Behaviour: How to Reduce Risk Through Employee Education, Training and Awareness*, 2nd ed. Routledge, 2022. [Online]. Available: https://www.taylorfrancis.com/books/9780429281785

[17] B. Alkhazi, M. Alshaikh, S. Alkhezi, and H. Labbaci, "Assessment of the Impact of Information Security Awareness Training Methods on Knowledge, Attitude, and Behavior," *IEEE Access*, vol. 10, pp. 132132 – 132143, 2022, doi: 10.1109/ACCESS.2022.3230286.

[18] H. A. Kruger and W. D. Kearney, "A prototype for assessing information security awareness," *Comput. Secur.*, vol. 25, no. 4, pp. 289–296, 2006, doi: 10.1016/j.cose.2006.02.008.

[19] K. R. Kont, "Information security awareness of librarians in the baltic countries: A comparative analysis," *Balt. J. Mod. Comput.*, vol. 11, no. 3, pp. 450–474, 2023, doi: 10.22364/bjmc.2023.11.3.07.

[20] N. J. MacKinnon and J. Hoey, "Operationalizing the Relation Between Affect and Cognition With the Somatic Transform," *Emot. Rev.*, vol. 13, no. 3, pp. 245–256, 2021, doi: 10.1177/17540739211014946.

[21] A. McCormac, T. Zwaans, K. Parsons, D. Calic, M. Butavicius, and M. Pattinson, "Individual differences and Information Security Awareness," *Comput. Human Behav.*, vol. 69, pp. 151–156, 2017, doi: 10.1016/j.chb.2016.11.065.

[22] T. Moletsane and P. Tsibolane, "Mobile Information Security Awareness among Students in Higher Education : An Exploratory Study," *2020 Conf. Inf. Commun. Technol. Soc. ICTAS 2020 - Proc.*, pp. 1–6, 2020, doi: 10.1109/ICTAS47918.2020.233978.

[23] D. S. Hermawan, F. Setiadi, and D. Oktaria, "Measurement Level of Information Security Awareness for Employees Using KAB Model with Study Case at XYZ Agency," in *2022 1st International Conference on Software Engineering and Information Technology (ICoSEIT)*, Nov. 2022, pp. 174–179. doi: 10.1109/ICoSEIT55604.2022.10029989.

[24] 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.

[25] U. Sekaran and R. Bougie, *Research Methods For Business: A Skill Building Approach*, Seventh Ed. Chichester, West Sussex, United Kingdom: John Wiley & Sons Ltd., 2016. [Online]. Available: https://www.wiley.com/en-gb/Research+Methods+For+Business%3A+A+Skill+Building+Approach%2C+7th+Edition-p-9781119266846

[26] N. M. Janna and H. Herianto, "Konsep Uji Validitas Dan Reliabilitas Dengan Menggunakan SPSS," *J. Darul Dakwah Wal-Irsyad*, no. 18210047, pp. 1–12, Jan. 2021, doi: 10.31219/osf.io/v9j52.

[27] S. L. Jackson, *Research Methods and Statistics: A Critical Thinking Approach*, 5th Ed. Boston: Cengage Learning, 2016. [Online]. Available: https://faculty.cengage.com/titles/9780357670934?q=contents