Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK) DOI: 10.25126/jtiik.20241128106
Vol. 11, No. 2, April 2024, hlm. 315-320 p-ISSN: 2355-7699
Akreditasi KEMENRISTEKDIKTI, No. 36/E/KPT/2019 e-ISSN: 2528-6579

PENGUKURAN KESADARAN KEAMANAN INFORMASI PEGAWAI: STUDI KASUS PT MESHINDO JAYATAMA

Abdul Gofur[*1], Rizal Fathoni Aji [2], Heri Kurniawan [3]

[1,2,3]Universitas Indonesia, Depok
Email: [1]abdul.gofur21@ui.ac.id, [2]rizal@cs.ui.ac.id, [3]herik@cs.ui.ac.id
[*]Penulis Korespondensi

(Naskah masuk: 22 November 2023, diterima untuk diterbitkan: 04 April 2024)

Abstrak

Integrasi teknologi dalam organisasi meningkatkan pertukaran informasi yang membuat organisasi lebih rentan terhadap serangan siber. Laporan Publik Hasil Monitoring Keamanan Siber Bulan April 2023 Badan Siber dan Sandi negara (BSSN) menyatakan terdapat 27.476.788 anomali trafik dan tertinggi adalah malware sebanyak 14.235.050. Serangan *cyber* juga dialami oleh PT Meshindo Jayatama yang memiliki data informasi penting sebagai aset dalam mendukung kegiatan usahanya. Hasil wawancara dengan Presiden Direktur dan Manager Teknologi Informasi (TI) PT Meshindo Jayatama menyatakan bahwa telah terjadi serangan seperti *Phishing* dan *Malware* sebanyak 26 kali ditahun 2023. Dengan adanya serangan *malware* yang mengakibatkan terinfeksinya dokumen laporan perusahaan dan kerugian finansial yang disebabkan oleh faktor kelalaian sumber daya manusia, menjadi pertimbangan perlu untuk dilakukan pengukuran kesadaran keamanan informasi dan mengetahui area yang perlu ditingkatkan. Penelitian ini menggunakan kuesioner sebagai metode pengumpulan data yang disusun berdasarkan *Human Aspects of Information Security Questionnaire* (HAIS-Q) dengan kerangka kerja *Knowledge Attitude Behavior* (KAB) dan penskalaan prioritas menggunakan *Analytic Hierarchy Process* (AHP). Hasil pengukuran kesadaran keamanan informasi pegawai PT Meshindo Jayatama berada dilevel "baik" dengan nilai 83,40%. Dari pengukuran tersebut, diketahui terdapat fokus area pada level "sedang" yaitu penggunaan perangkat *mobile* dan pengelolaan *password*. selanjutnya, Peneliti memberikan saran untuk diselenggarakan program pelatihan keamanan informasi dengan media yang menarik dan dilakukan secara berkelanjutan dan perlu diterapkan atau diperbaharui seluruh kebijakan terkait keamanan informasi perusahaan.

Kata kunci: *kesadaran keamanan informasi, Human Aspects of Information Security Questionnaire (HAIS-Q), Analytical Hierarchy Process (AHP)*

MEASUREMENT OF EMPLOYEE INFORMATION SECURITY AWARENESS: A CASE STUDY OF PT MESHINDO JAYATAMA

Abstract

The integration of technology in organizations increases the exchange of information making organizations more vulnerable to cyber attacks. Public Report on Cyber Security Monitoring Results for April 2023, the National Cyber and Crypto Agency (BSSN) stated that there were 27,476,788 traffic anomalies and the highest was malware at 14,235,050. Cyber attacks were also experienced by PT Meshindo Jayatama, which has important information data as assets to support its business activities. The results of interviews with the President Director and Information Technology (IT) Manager of PT Meshindo Jayatama stated that attacks such as Phishing and Malware had occurred 26 times in 2023. These malware attacks resulted in the infection of company report documents and financial losses caused by human resource negligence, it is necessary to measure information security awareness and identify areas that need to be improved. In this research, a questionnaire was used as a data collection method which was prepared based on the Human Aspects of Information Security Questionnaire (HAIS-Q) with the Knowledge Attitude Behavior (KAB) framework and priority scaling using the Analytic Hierarchy Process (AHP). The results of measuring the information security awareness of PT Meshindo Jayatama employees were at the "good" level (83.40%). There is a focus area at the "medium" level, namely the use of mobile devices and password management. Researchers provide suggestions for holding security training programs with interesting media and carried out on an ongoing basis and need to implement or update all policies related to company information security.

Keywords: *information security awareness, Human Aspects of Information Security Questionnaire (HAIS-Q), Analytical Hierarchy Process (AHP)*

1. PENDAHULUAN

Dalam dunia digital yang semakin berkembang, keamanan sistem informasi adalah bagian yang penting untuk organisasi. Organisasi perlu melindungi aset sistem informasinya dari serangan berbahaya, seperti *ransomware*, *malware*, dan serangan siber lainnya (Khando et al., 2021). Selain itu, Integrasi teknologi dalam organisasi meningkatkan pertukaran informasi yang membuat organisasi lebih rentan terhadap serangan siber seperti kejahatan terorganisir yang bertujuan untuk pemalsuan konten, pemantauan aliran informasi, gangguan basis data, dan pelanggaran hak kekayaan intelektual (Hassanzadeh, Jahangiri and Brewster, 2014).

Ancaman akan kerentanan lingkungan pertukaran informasi tersebut dibuktikan oleh data yang disajikan Badan Siber dan Sandi negara (BSSN) pada Laporan Bulanan Publik Hasil Monitoring Keamanan Siber periode April 2023 yang menyebutkan bahwa terdapat 27.476.788 anomali trafik di bulan April 2023. Jumlah tertinggi terjadi pada 18 April 2023 sebanyak 1.600.334 anomali trafik. Klasifikasi tertinggi dari anomali yang terjadi adalah malware yang mencapai 14.235.050. 5 jenis malware terbanyak adalah *Generic Trojan RAT activity, PhishingSite Other Malware Activity, Discover the communication behavior of vpn tool openvpn, MiningPoolMining Virus, dan CobaltStrike RAT activity* (BSSN., 2023).

Ancaman akan serangan juga dialami oleh PT Meshindo Jayatama yang memiliki aset dan data informasi yang penting dalam mendukung kegiatan usahanya. PT Meshindo Jayatama merupakan perusahaan yang bergerak dibidang penyediaan komponen elektrikal untuk industri otomasi sejak tahun 2009 dan fokus pada perdagangan komponen kelistrikan untuk berbagai pelanggan industri. Perusahaan ini merupakan distributor resmi dan pusat layanan Yaskawa *Inverter* yang didukung penuh oleh PT Yaskawa Electric Indonesia (Meshindo., 2023). Berdasarkan hasil wawancara dengan Presiden Direktur dan Manager TI PT Meshindo Jayatama juga menyatakan bahwa telah terjadi serangan seperti *Phishing* dan *Malware* sebanyak 26 kali ditahun 2023 hingga periode 15 Septermber 2023. Atas serangan tersebut, disampaikan bahwa terdapat 2 kejadian serangan *malware* yang mengakibatkan beberapa dokumen laporan perusahaan terinfeksi sehingga memberikan dampak kerugian secara finansial kepada PT Meshindo Jayatama. Selanjutnya, PT Meshindo Jayatama telah meningkatkan upaya preventif atas kejadian serupa dimasa mendatang dengan meningkatkan pengaturan keamanan teknologi yang diterapkan. Akan tetapi, walaupun penanggulangan, teknologi memberikan kontribusi dalam menjadi solusi yang efektif, tetapi tidak sepenuhnya dapat menangani semua risiko keamanan informasi, dan sumber daya manusia dalam organisasi pada kenyataannya merupakan garis pertahanan utama dan menentukan (Hassanzadeh, Jahangiri and Brewster, 2014).

Berdasarkan hal-hal tersebut diatas dan mempertimbangkan eksposur risiko finansial dan reputasi yang mungkin dihadapi PT Meshindo Jayatama jika terdampak oleh serangan keamanan informasi yang disebabkan oleh faktor kelalaian sumber daya manusia, diperlukan penelitian untuk mengukur tingkat kesadaran keamanan informasi dan mengetahui "Sejauh mana tingkat kesadaran keamanan informasi keamanan informasi pegawai PT Meshindo Jayatama?".

Berbagai penelitian terkait pengukuran kesadaran keamanan informasi telah dilakukan oleh beberapa peneliti yaitu Mainar Swari Mahardika dkk (2020) yang melakukan penelitian terkait pengukuran kesadaran keamanan informasi di Pusat Analisis dan Pelayanan Informasi Komisi Yudisial Republik Indonesia. Penelitian ini melakukan pengukuran kesadaran keamanan informasi dengan menggunakan metode HAIS-Q berdasarkan kerangka kerja *Knowledge Attitude Behavior* (KAB) dikembangkan oleh Kruger dan Kearney dan penskalaan prioritas fokus area menggunakan AHP (Mahardika et al., 2020).

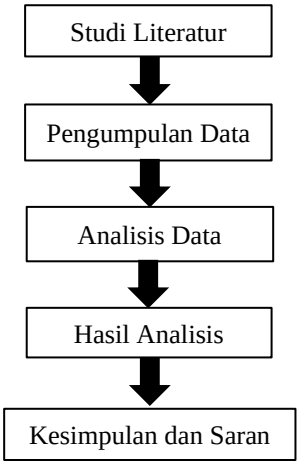
Pendekatan metode dan penskalaan prioritas fokus area yang serupa juga dilakukan oleh Halida Ernita dkk (2022) dalam penelitian terkait Strategi Peningkatan *Security Awareness* Pegawai Direktorat Teknologi Informasi Bank XYZ khususnya Direktorat TI (Ernita et al., 2022). Metode Pendekatan berbeda dilakukan oleh Kusumawati (2018) dalam penelitiannya yang mengukur kesadaran keamanan Informasi pada Studi kasus di pemerintahan. Penelitian ini juga menggunakan kerangka kerja KAB dikembangkan oleh Kruger dan Kearney. Akan tetapi, pengukuran berdasarkan *Multiple Criteria Decision Analysis* (MCDA) untuk melakukan pengukuran nilai alternatif yang didasari kriteria tertentu (Kusumawati, 2018). Achmad Tarmizi dkk (2018) dalam penelitian terkait pengukuran kesadaran keamanan informasi di Badan Tenaga Nuklir Nasional (BATAN). Pada penelitian tersebut dilakukan *Focus Group Discussion* (FGD) untuk menentukan penskalaan prioritas fokus area yang kemudian dituangkan kedalam kuesioner dan selanjutnya digunakan *regression analysis* untuk pengukurannya (Tarmizi et al., 2019).

Berdasarkan penelitian terkait sebelumnya tersebut diatas, peneliti akhirnya memilih mengukur kesadaran keamanan informasi dengan menggunakan metode HAIS-Q berdasarkan kerangka kerja KAB dengan pertimbangan dapat dirumuskan lebih spesifik (Kruger and Kearney, 2006) dan penskalaan prioritas fokus area menggunakan AHP karena keunggulannya dalam pengukuran menggunakan perbandingan berpasangan telah divalidasi oleh penilaian ahli. Selain itu, pengukuran dengan AHP dapat menampilkan hasil yang lebih konsisten, mudah digunakan dan dipahami (Saaty, 2008).

Selanjutnya, berdasarkan hasil penelitian terkait pengukuran tingkat kesadaran keamanan tersebut dihasilkan kesimpulan dan saran yang diharapkan dapat meningkatkan kesadaran keamanan Informasi pegawai PT Meshindo Jayatama di area yang dirasa belum maksimal.

2. METODE PENELITIAN

Peneliti melakukan 5 tahapan proses dalam metode penelitian yaitu sebagai berikut:



Gambar 1. Metode Penelitian

2.1 Studi Literatur

Peneliti melakukan penelaahan terhadap penelitian yang pernah dilakukan oleh Peneliti sebelumnya dan melakukan pencarian literatur atau melakukan peninjauan pustaka terhadap penelitian yang akan dilakukan. Adapun beberapa tinjauan literatur yang digunakan dalam penelitian ini yaitu:

a) *Information Security Awareness* (ISA)

Menurut Bulgucru (2010), *Information Security Awareness* atau kesadaran keamanan informasi didefinisikan sebagai keseluruhan pengetahuan dan pemahaman pegawai tentang masalah potensial yang terkait dengan keamanan informasi dan kesadarannya terhadap Kebijakan Keamanan Informasi organisasinya (Bulgurcu, Cavusoglu and Benbasat, 2010). Menurut Siponen (2000) , memahami ISA dan faktor penyebabnya sangat penting dalam mengurangi risiko keamanan informasi. ISA mengacu pada sejauh mana pegawai memahami pentingnya aturan, kebijakan, dan pedoman keamanan informasi organisasi mereka, dan berperilaku sejalan dengan kebijakan, aturan, dan pedoman tersebut (Siponen, 2000). Menurut Parson dkk (2014), kesadaran keamanan informasi berfokus terhadap dua aspek, yaitu pertama batasan sejauh mana pegawai memahami perilaku keamanan Informasi yang didasarkan pada aturan terkait keamanan informasi. Kedua, sejauh mana pegawai memiliki komitmen dan berperilaku sesuai dengan peraturan dan kebijakan yang ada (Parsons et al., 2014).

b) *Human Aspect of Information Security Awareness Questionnaire* (HAIS-Q).

HAIS-Q dikembangkan oleh Parson dkk (2014) dengan berbasis kerangka KAB yang dikembangkan oleh Kruger dan Kearney (2006) untuk mengukur tiga aspek yang meliputi pengetahuan, sikap, dan perilaku (Kruger and Kearney, 2006). Pada HAIS-Q, aspek pengetahuan, sikap, dan perilaku diukur dan dievaluasi untuk menjaga keeimbangan antara ukuran spesifik area yang paling penting untuk membatasi kuesioner. Pengukuran ISA dengan HAIS-Q memiliki 63 sub-area yang dikategorisasikan menjadi 7 fokus area yaitu pengelolaan password, penggunaan internet, penggunaan email, penggunaan perangkat mobile, penggunaan media sosial, pelaporan insiden dan penanganan informasi (Parsons et al., 2014).

c) Analytic Hierarchy Process (AHP)

Menurut Saaty, AHP adalah teori pengukuran untuk memperoleh skala prioritas yang dinilai oleh para ahli dengan dengan menggunakan perbandingan berpasangan. AHP menyediakan kerangka komprehensif dan rasional untuk mengukur unsur, menghubungkan elemen dengan tujuan keseluruhan, dan untuk mengevaluasi alternatif solusi (Saaty, 2008)

2.2 Pengumpulan Data

Setelah melakukan studi literatur, Peneliti mengumpulkan data dengan menggunakan kuesioner yang disusun menggunakan HAIS-Q sebagai acuan dengan 7 fokus area yaitu pengelolaan *password*, penggunaan internet, penggunaan *email*, penggunaan perangkat *mobile*, penggunaan media sosial, pelaporan insiden dan penanganan informasi. Pengisian kuesioner ini dilakukan menggunakan *Google Form* secara *online* dan diberikan kepada pada pegawai di PT Meshindo Jayatama.

Kuesioner yang diberikan berisi 63 pertanyaan yang meliputi tiga pertanyaan untuk masing-masing *sub area* yang meliputi aspek pengetahuan (*Knowledge*), sikap (*Attitude*), dan perilaku (*Behavior*). Responden akan diminta untuk menjawab dengan 5 pilihan jawaban yang merujuk Skala Likert:

1 = Sangat Tidak Setuju
2 = Tidak Setuju
3 = Netral
4 = Setuju
5 = Sangat Setuju

Sebagai contoh, *sub area* “menggunakan kombinasi huruf, simbol, dan angka sebagai kombinasi password” terdiri dari 3 pertanyaan yang meliputi aspek pengetahuan, sikap, dan perilaku sebagaimana pada tabel 1.

Tabel 1. Contoh pertanyaan berdasarkan aspek KAB

aspek	pertanyaan
Pengetahuan (K)	Saya merasa harus menggunakan kombinasi huruf, simbol, dan angka sebagai kombinasi password
Sikap (A)	Saya tidak khawatir hanya menggunakan huruf dalam kombinasi password yang saya miliki
Perilaku (B)	Saya telah menggunakan kombinasi huruf, simbol, dan angka sebagai kombinasi password

Jumlah sampel responden yang diambil dihitung menggunakan rumus Slovin (Ryan Jr. and Ryan, 2013) sebagaimana persamaan (1) berikut:

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

n = jumlah sampel yang dibutuhkan yaitu 24,24 (dibulatkan menjadi 25) dengan N = total populasi yaitu jumlah pegawai sebanyak 32, e = *error level* (biasanya berkisar 1%, 5%, atau 10% yang dapat ditentukan oleh peneliti) yaitu 10%.

Total Pegawai pada PT Meshindo Jayatama adalah 32 orang yaitu terdiri atas 1 orang Presiden Direktur, 4 orang Manajer, 5 orang *Supervisor* dan 22 orang pegawai setingkat staf seperti pada tabel 2.

Tabel 2. Jumlah Pegawai PT Meshindo Jayatama

jabatan	jumlah
Presiden Direktur	1 orang
Manajer	4 orang
Supervisor	5 orang
Setingkat Staf	22 orang

Selain pengisian kuesioner, Peneliti juga melakukan wawancara kepada Manajer TI untuk menentukan prioritas dari 7 fokus area menggunakan metode AHP. Metode AHP mengharuskan untuk dilakukan perbandingan berpasangan (*pair comparison)* atas tiap-tiap kriteria area kesadaran keamanan Informasi. Berdasarkan hasil wawancara, diperoleh matriks yang membandingkan beberapa alternatif berdasarkan kriteria tertentu. Skala perbandingan yang digunakan adalah 1 hingga 9, dengan 1 memperlihatkan tingkatan kepentingan yang paling rendah rendah (*equal importance*) dan 9 memperlihatkan tingkat kepentingan yang paling tinggi (*extreme importance*). Hasil dari komparasi tersebut sebagaimana pada tabel 3.

Tabel 3. Penentuan Skala Prioritas Fokus Area menggunakan Metode AHP

kriteria A	kriteria B	lebih penting A atau B?	skala (1-9)
Pengelolaan *Password*	Penggunaan *email*	A	3
	Penggunaan internet	A	3
	Penggunaan media sosial	A	3
	Penggunaan perangkat *mobile*	A	2
	Penanganan informasi	A	5
	Pelaporan insiden	A	5
Penggunaan *email*	Penggunaan internet	B	2
	Penggunaan media sosial	A	2
	Penggunaan perangkat *mobile*	B	3
	Penanganan informasi	A	5
	Pelaporan insiden	A	5
Penggunaan internet	Penggunaan media sosial	A	2
	Penggunaan perangkat *mobile*	B	3
	Penanganan informasi	A	5
	Pelaporan insiden	A	5
Penggunaan media sosial	Penggunaan perangkat *mobile*	B	3
	Pelaporan insiden	A	5
	Penanganan informasi	A	3
Penggunaan perangkat *mobile*	Penanganan informasi	A	3
	Pelaporan insiden	A	5
Penanganan informasi	Pelaporan insiden	A	3

2.3. Analisis Data

Langkah pertama yang dilakukan untuk mendapatkan nilai tingkat kesadaran keamanan informasi melalui metode HAIS-Q adalah mengidentifikasi pertanyaan yang memiliki makna positif dan pertanyaan yang mengandung makna negatif. Untuk setiap pertanyaan positif, skor 1 diberikan untuk jawaban pada skala 4 dan 5 dan nilai 0 untuk jawaban pada skala 1 sampai 3. Sebaliknya, untuk pertanyaan negatif, skor 1 diberikan untuk jawaban dengan skala 1 dan 2 dan nilai 0 untuk jawaban dengan skala 3 sampai dengan 5. Setelah mendapatkan skor 1 dan 0, langkah selanjutnya adalah menjumlahkan semua jawaban dengan nilai 1 dan 0 untuk setiap pertanyaan. Hasil yang diperoleh digunakan sebagai nilai persentase dengan membagi jumlah responden. Angka ini menjadi nilai untuk satu dimensi sub-area. Untuk mendapatkan nilai suatu fokus area, maka setiap nilai dimensi pada suatu fokus area dikalikan dengan bobot dimensi seperti yang didefinisikan oleh Kruger dan Kearney (Kruger and Kearney, 2006) pada tabel 4.

Tabel 4. Dimensi Pembobotan

dimensi	bobot
Pengetahuan (K)	30
Sikap (A)	20
Perilaku (B)	50

Langkah selanjutnya adalah menghitung nilai tingkat kesadaran keamanan informasi dengan mengalikan hasil tiap fokus area (v_i) dengan bobot tiap fokus area (w_i) yang telah dibuat dengan tim pakar sebelumnya menggunakan rumus persamaan (2) sebagai berikut (Kruger and Kearney, 2006):

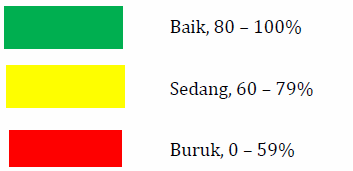
$$V(a) = \sum_{i=1}^{n} v_i\ (a)\ w_i \qquad (2)$$

Perhitungan bobot dengan metode AHP untuk setiap fokus area sebagaimana pada tabel 5.

Tabel 5. Bobot Untuk Setiap Fokus Area

fokus area	bobot
Pengelolaan *Password*	30.04%
Penggunaan *Email*	13.12%
Penggunaan Internet	15.42%
Penggunaan Media Sosial	9.88%
Penggunaan Perangkat *Mobile*	23.14%
Penanganan Informasi	5.19%
Pelaporan Insiden	3.20%

Hasil perhitungan bobot akan digunakan untuk menghitung nilai tingkat kesadaran keamanan informasi dari hasil kuesioner yang telah dibagikan. Skor tersebut akan dipetakan menjadi tiga level yaitu buruk (*bad*), sedang (*medium*), dan baik (*good*) yang mengacu berdasarkan jurnal Kruger dan Kearney (Kruger and Kearney, 2006) dan dapat dilihat pada Gambar 2.



Gambar 2. Skala Tingkat kesadaran keamanan informasi Keamanan Informasi

3. HASIL DAN PEMBAHASAN

Berdasarkan hasil kuesioner yang telah dibagikan kepada Pegawai di PT Meshindo Jayatama, jumlah responden yang mengisi kuesioner tersebut sebanyak 28 pegawai. Hal ini telah mencukupi dari minimal jumlah sample yang dibutuhkan sebelumnya yaitu sebesar 25 pegawai. Data responden penelitian ditunjukkan pada tabel 5.

Tabel 5. Data Responden

karakteristik		jumlah
Usia	20 - 30 tahun	8
	31 - 40 tahun	12
	41 - 50 tahun	4
	Diatas 50 tahun	4
Jenis Kelamin	Laki-Laki	16
	Perempuan	12
Jabatan	Presiden Direktur	1
	Manajer	4
	Supervisor	5
	Staf - setingkat	18
Tingkat Pendidikan	S2	3
	S1	14
	D3	7
	SMA	4

Tabel 5 memperlihatkan data responden dengan karakteristik jenis kelamin, usia, jabatan dan tingkat pendidikan. Berdasarkan tabel tersebut diketahui jumlah laki-laki sedikit lebih banyak dari perempuan. Rentang usia terbanyak adalah 31-40 tahun, jabatan terbanyak responden adalah setingkat staf, dan tingkat pendidikan terbanyak responden adalah S1.

Berdasarkan hasil pengukuran rata-rata tingkat kesadaran keamanan informasi pegawai PT Meshindo Jayatama, diperoleh total nilai sebesar 84,43% yang berarti kesadaran pegawai PT Meshindo Jayatama berada pada level "baik" sebagaimana pada tabel 6.

Tabel 6. Tingkat Kesadaran Keamanan Informasi

fokus area	pengetahuan	sikap	perilaku	total
Pengelolaan *Password*	86.90%	75.00%	84.52%	83.33%
Penggunaan *Email*	95.24%	86.90%	96.43%	94.17%
Penggunaan Internet	85.71%	91.67%	91.67%	89.88%
Penggunaan Media Sosial	89.29%	92.86%	90.48%	90.60%
Penggunaan Perangkat *Mobile*	61.90%	73.81%	78.57%	72.62%
Penanganan Informasi	84.52%	84.52%	84.52%	84.52%
Pelaporan Insiden	90.48%	97.62%	96.43%	94.88%
Total	81.91%	80.43%	85.49%	84.43%

4. KESIMPULAN DAN SARAN

Pengukuran kesadaran keamanan informasi di PT Meshindo Jayatama telah dilakukan terhadap penerapan aspek pengetahuan, sikap, dan perilaku pegawai pada 7 fokus area yang terdiri dari pengelolaan *password*, penggunaan internet, penggunaan *email*, penggunaan perangkat *mobile*, penggunaan media sosial, pelaporan insiden dan penanganan informasi.

Secara umum tingkat kesadaran keamanan Informasi pegawai PT Meshindo Jayatama telah berada dilevel "baik" dengan persentase 84,43%. Untuk menjaga dan meningkatkan level tersebut, peneliti merekomendasikan untuk menerapkan atau memperbaharui seluruh kebijakan terkait keamanan informasi perusahaan dan secara berkelanjutan menyelenggarakan sosialisasi, pendidikan dan pelatihan terkait program kesadaran keamanan informasi yang dilengkapi dengan program dan media yang menarik dan beragam serta melakukan pembaharuan secara rutin terkait sistem operasi, aplikasi, perangkat lunak, anti-virus, dan perangkat keamanan sistem. Selain itu, berdasarkan hasil pengukuran kesadaran keamanan informasi, terdapat fokus area yang berada pada level "sedang" yaitu sebagai berikut:

a) Pengelolaan *password*

Dalam fokus area ini, aspek sikap berada di level sedang dengan nilai 75%. Komponen utama yang membuat penilaian ini rendah yaitu pegawai cenderung tidak menggunakan huruf, angka dan karakter dalam kombinasi *password* yang digunakan dan menggunakan *password* yang sama untuk media sosial dan akun yang

digunakan dalam bekerja. Terkait hal tersebut, peneliti merekomendasikan untuk menerapkan kebijakan yang mengatur keamanan *password* yang mewajibkan pegawai untuk menggunakan kombinasi huruf, angka dan karakter serta minimal 8 karakter dan penggantian *password* secara berkala.

b) Pemakaian perangkat *mobile*

Dalam fokus area ini, ketiga aspek baik pengetahuan, sikap dan perilaku masih berada di level sedang. Komponen utama yang membuat penilaian ini rendah yaitu pegawai cenderung masih melakukan pengiriman file dokumen sensitif perusahaan dengan menggunakan *laptop* sebagai perangkat *mobile* dengan *wifi* umum. terkait hal tersebut, peneliti merekomendasikan untuk membuat dan menerapkan kebijakan yang mengatur pemakaian perangkat *mobile*, termasuk prosedur yang mencegah penggunaan *wifi* umum untuk tujuan pekerjaan. Selain itu, diperlukan pengaturan terkait penggunaan VPN untuk pegawai yang ingin mengakses dokumen atau *email* kantor dari luar.

DAFTAR PUSTAKA

BSSN. 2023. Monitoring Keamanan Siber 2023 | www.bssn.go.id. [online] Tersedia melalui: <https://www.bssn.go.id/monitoring-keamanan-siber-2023/> [Diakses 29 September 2023].

MESHINDO. 2023. PT. MESHINDO JAYATAMA – About Us. [online] Tersedia melalui: <https://www.meshindo-jayatama.com/about-us> [Diakses 29 September 2023].

BULGURCU, B., CAVUSOGLU, H. AND BENBASAT, 2010. Special issue information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Quarterly, 34(3), 523–548. https://doi.org/10.2307/25750690

ERNITA, H., RULDEVIYANI, Y., NURUL MAFTUHAH, D. AND MULYADI, R., 2022. Strategy to Improve Employee Security Awareness at Information Technology Directorate Bank XYZ. Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi), 6(4), pp.577–584. https://doi.org/10.29207/resti.v6i4.4170.

HASSANZADEH, M., JAHANGIRI, N. AND BREWSTER, B., 2014. A Conceptual Framework for Information Security Awareness, Assessment, and Training. Emerging Trends in ICT Security, pp.99–110. https://doi.org/10.1016/B978-0-12-411474-6.00006-2.

KHANDO, K., GAO, S., ISLAM, S.M. AND SALMAN, A., 2021. Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security*, 106, p.102267. https://doi.org/10.1016/J.COSE.2021.102267.

KRUGER, H.A. AND KEARNEY, W.D., 2006. A prototype for assessing information security awareness. *Computers & Security*, 25(4), pp.289–296. https://doi.org/10.1016/J.COSE.2006.02.008.

KUSUMAWATI, A., 2018. *Information Security Awareness: Study on a Government Agency*. IEEE.

MAHARDIKA, M.S., HIDAYANTO, A.N., PARAMARTHA, P.A., OMPUSUNGGU, L.D., MAHDALINA, R. AND AFFAN, F., 2020. Measurement of employee awareness levels for information security at the center of analysis and information services judicial commission Republic of Indonesia. *Advances in Science, Technology and Engineering Systems*, 5(3), pp.501–509. https://doi.org/10.25046/aj050362.

PARSONS, K., MCCORMAC, A., BUTAVICIUS, M., PATTINSON, M. AND JERRAM, C., 2014. Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers and Security*, 42, pp.165–176. https://doi.org/10.1016/j.cose.2013.12.003.

RYAN JR., T.P. AND RYAN, T.P., 2013. *Sample Size Determination and Power*. [online] Newark, UNITED STATES: John Wiley & Sons, Incorporated. Tersedia melalui: <http://ebookcentral.proquest.com/lib/indonesiau-ebooks/detail.action?docID=1207569>.

SAATY, T.L., 2008. Decision making with the analytic hierarchy process. International Journal of Services Sciences (IJSSCI), pp.83–95. https://doi.org/10.1504/IJSSCI.2008.017590

SIPONEN, M.T., 2000. A conceptual foundation for organizational information security awareness. Information Management & Computer Security, Vol.8 No. 1, pp.31-41.

TARMIZI, A., HAPSARI, I.C., HIDAYANTO, A.N., ADHI YUNIARTO, L.Y. AND HERKULES, 2019. Information security awareness national nuclear energy agency of Indonesia (BATAN). Institute of Electrical and Electronics Engineers Inc. pp.35–39. https://doi.org/10.1109/ICCED.2018.00017.