Pengukuran Tingkat Kesadaran Keamanan Pegawai Divisi Ict Perusahaan Minyak X Di Indonesia

Measuring The Security Awareness Level Of Ict Division Employees At Oil Company X In Indonesia

Imam Ryan Maulana[1], Candiwan[2]
[1] Manajemen Bisnis Telkomunikasi dan Informatika, Fakultas Ekonomi dan Bisnis, Universitas Telkom, Indonesia, Imamryannst@student.telkomuniversity.ac.id
[2] Manajemen Bisnis Telkomunikasi dan Informatika, Fakultas Ekonomi dan Bisnis, Universitas Telkom, Indonesia, candiwan@telkomuniversity.ac.id

Abstract
Information system security awareness is very important in this modern era and the rapid development of technology, the use of information systems is also used in various large companies, not only to assist in running a business, but also to be used as an environment for doing work. It is not only technology-based companies that take advantage of technology and the times, but large companies engaged in the oil and gas sector, such as Company X, also use technology as a vehicle for carrying out and carrying out their work. The complexity of the problem of information security is divided into two, namely system security and user security. Every company certainly has demands in obtaining, storing, managing and guaranteeing the confidentiality and security of company data, in order to ensure the continuity of the company's business activities. However, from the information the author got about company X, until now there are still many incidents of information security that stem from employee negligence. Such as finding employees trapped in phishing e-mail simulations. This study aims to determine the level of information security management awareness of employees of the ICT division of oil company X in Indonesia. The research was conducted by distributing questionnaires to employees of the ICT division of company X. The questionnaire was developed using the Human Aspect of Information System Questionnaire (HAIS-Q) with seven focus areas in each dimension of knowledge, attitude and behavior. Data analysis uses the Analytical Hierarchy Process (AHP). The results of the study showed that the employees of division X were in the "good" category.

Keywords-Information Security, Oil and Gas Company, Information security management.

Abstrak
Kesadaran keamanan *system* informasi sangatlah penting di era yang serba modern dan perkembangan teknologi yang semakin cepat, penggunaan *system* informasi juga digunakan di berbagai perusahaan besar, tidak hanya untuk membantu dalam menjalankan bisnis, namun juga dapat digunakan sebagai *environment* dalam melakukan pekerjaan. Tidak hanya pada perusahaan yang memang berbasiskan teknologi saja yang menggunakan keuntungan dari teknologi dan perkembangan zaman, namun perusahaan besar yang bergerak di bidang MIGAS layaknya Perusahaan X ikut turut menggunakan teknologi sebagai wadah dalam melakukan dan melaksanakan pekerjaannya. Kompleksitas dari permasalahn keamanan informasi dibagi menjadi dua, yaitu keamanan *system* dan pengguna. Tiap perusahaan tentunya memiliki tuntutan dalam mendapatkan, menyimpan, mengelola dan menjamin kerahasiaan serta keamanan data perusahaan, demi menjamin kelangsungan aktivitas bisnis perusahaan. Namun, dari informasi yang di dapat penulis mengenai perusahaan X, hingga saat ini masih banyak ditemukan insiden-insiden dari keamanan informasi yang berasal dari kelalaian pegawai. Seperti temuan terjebaknya pegawai dalam simulasi email *phising*. Penelitian ini bertujuan untuk mengetahui tingkat kesadaran manajemen keamanan informasi dari pegawai divisi ICTtperusahaannminyak X di Indonesia. Penelitian dilakukan dengan cara menyebarkannkuisioner kepada pegawai divisi ICT perusahaan X. kuisioner dikembangkan dengan menggunakan *Human Aspect of Information System Questionnaire* (HAIS-Q) dengan tujuh area fokus di setiap dimensi *knowledge*, *attitude*, *and behavior*. Analisis data menggunakan *Analytical Hierarchy Process* (AHP). Hasil peneletian menunjukan bahwa pegawai divisi X dalam kategori "*good*".

Kata Kunci-Keamanan Informasi, Perusahaan MIGAS, Manajemen keamanan informasi.

I. PENDAHULUAN

Seriring berjalannya waktu, Perkembangan teknologi informasi semakin lama berkembang dengan sangat pesat. Perkembangan ini dapat memberikan dampak positif bagi semua orang dan bidang pekerjaan. Kemajuan teknologi ini tentunya akan sangat membantu pekerjaan dan kehidupan masyarakat jika digunakan dengan baik dan benar, namun apabila ada kelebihan tentunya pasti juga ada kekurangan. Dampak yang harus diperhatikan dari penggunaan teknologi informasi untuk bisnis salah satunya ialah masalah keamanan.

Manajemen keamanan informasi merupakan bagian penting dari keamanan *cyber*. Dalam kerangka COBIT (*Control Objective for Information and Related Technology*), keamanan informasi sangat penting dalam menjaga privasi data yang tidak dapat dipublikasikan. Selain COBIT, framework ISO/IEC 27001 juga mengevaluasi komponen keamanan informasi dari sistem informasi yang digunakan oleh institusi. Perlu adanya tata kelola manajemen yang baik untuk mengklasifikasikan berbaga risiko yang berpotensi merugikan perusahaan. Pembahasan dalam penelitian ini akan dibahas mengenai menggambarkan perspektif dari karyawan salah satu perusahaan minyak yang ada di Indonesia untuk menjaga kelangsungan usaha dan melindungi data atau informasi yang bersifat rahasia (Singgalen et al., 2021)

Dilansir dari sumber *article* berita Bloomberg (Brambilla, 2022), perusahaan besar multinasional asal italia, mengalami percobaan *hack*. Telah dikonfirmasi bahwa *internal protection* telah mendeteksi percobaan akses oleh pikah yang tidak memiliki wewenang. Orang-orang yang mengetahui situasi tersebut mengatakan bahwa Eni telah terkena serangan *ransomware*. *Ransomware* merupakan sejenis *malware* yang mengunci komputer serta memblokir akses ke file sebagai pengganti pembayaran. Masih tidak jelas siapa yang bertanggung jawab atas pelanggaran tersebut. (IBM, 2014) menyatakan meskipun 45% serangan yang terjadi dilakukan dari pihak luar, namun 55% juga disebabkan dari pihak dalam yaitu mereka yang memiliki akses ke dalam suatu organisasi, atau karyawan yang kurang memiliki kesadaran keamanan informasi sehingga dapat menyebabkan insiden pada keamanan informasi.

Dilansir dari *CyberEdge's 2018 Cyberthreat Defense Report*, ketertakutan terbesar dari sebuah organisasi adalah kurangnya kesadaran keamanan karyawan. Karyawan yang kurang menyadari kewajiban dan kepentingan keamanan siber cenderung mengabaikan kebijakan dan prosedur yang relevan, yang dapat menyebabkan pengungkapan data yang tidak disengaja atau mengundang serangan siber dari luar yang berhasil. Seperti *phising* dan *ransomewere.* (Luke Irwin, n.d.). Berita tersebut membuktikan bahwa kejahatan teknologi informasi tidak hanya serangan dari luar saja yang berbahaya, namun kesadaran keamanan system dari pegawai juga menjadi poin penting dalam keberlangsungan kemanan suatu organisasi atau perusahaan. Setiap pengguna dan karyawan dari sebuah organiasi atau perusahaan, wajib bertanggung jawab atas penggunaan sumber daya yang diberikan secara aman. Untuk itu, pengguna harus bertindak setiap saat dengan mematuhi kode etik dari perusahaan, dan harus menghindari semua penyalahgunaan layanan atau bertentangan dengan kode etik dari peraturan yang telah ditetapkan. Dengan begitu peneliti ingin menelusuri tingkat kesadaran bagian internal dari sebuah divisi ICT pada suatu perusahaan MIGAS X terkait keamanan informasi.

II. DASAR TEORI DAN METODOLOGI

A. Manajemen Keamanan Informasi

Manajemen keamanan informasi merupakan cara untuk mengamankan aset informasi dari ancamam yang dapat mengancam dan menggangu. Informasi adalah *asset* yang sangat berharga dikarenakan hal tersebut adalah salah satu sumber daya strategis untuk meningkatkan nilai perusahaan serta kepercayaan masyarakat. Oleh karena itu, pentingnya melakukan dan memperhatikan perlindungan terhadap informasi (*security information*). Dengan memperhatikan keamanan informasi, maka perusahaan dapat terhindar dari pembobolan atau ancaman yang dapat terjadi. (Irwin, 2022).

B. Kesadaran Keamanan Informasi

Untuk kesadaran keamanan informasi bisa disebabkan oleh 3 hal, diantaranya ada sikap, pengetahuan, dan juga perilaku. Dalam konteks pengetahuan, pengguna *system* seperti pegawai bisa berguna dalam mempertimbangkan keamanan informasi sebelum menggunakan perangkat digital sebagai sarana transaksi bisnis atau *platform* pemasaran digital (Munthe & Purnama, 2019).

C. *Human Aspects of Information Security Questionnaire*

Human Aspects of Information Security Questionnaire (HAIS-Q) merupakan alat yang efektif dalam mengukur *information system awareness* (Parsons et al., 2017) menurut (Mahardika et al., 2020) HAIS-Q juga dirasa mampu untuk mengukur pengetahuan, sikap, serta perilaku dari individu yang mengenai hal sistem informasi menggunakan komponen knowledge, attitude, dan behavior

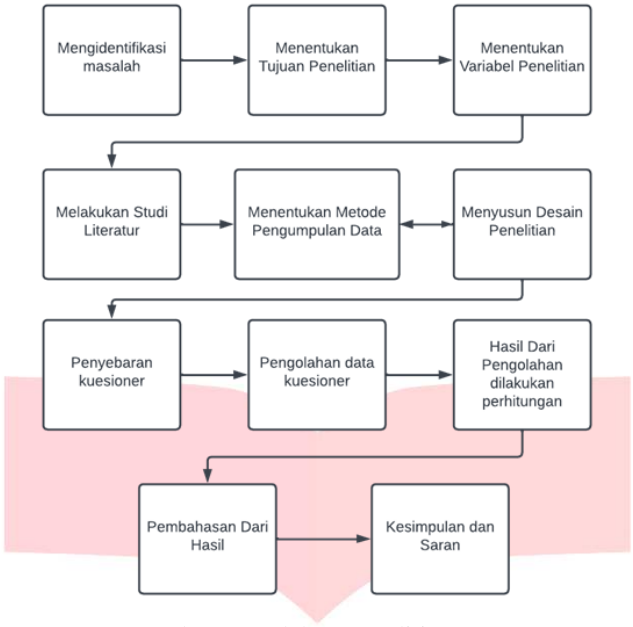
D. *Analytic Hierarchy Process (AHP)*

AHP adalah prosedur yang berbasis matematis yang sangat baik dan sesuai untuk kondisi evaluasi atribut-atribut kualitatif. AHP memiliki kelebihan dibandingkan yang lainnya karena adanya struktur yang berhirarki, sebagai konsekuensi dari kriteria yang dipilih, sampai kepada sub-sub kriteria yang paling mendetail (Makkasau, 2012).

E. Metode Penelitian

1. Tahap Penelitian

Peneliti melakukan penelitian dengan tahapan identifikasi masalah yang kemudian dilanjutkan ke tahap berikutnya hingga penarikan kesimpulan dan saran. Peneliti melakukan hal tersebut untuk membantu dalam mempermudah peneliti dalam melaksanakan penelitian. Berikut tahapan yang dilakukan oleh peneliti.

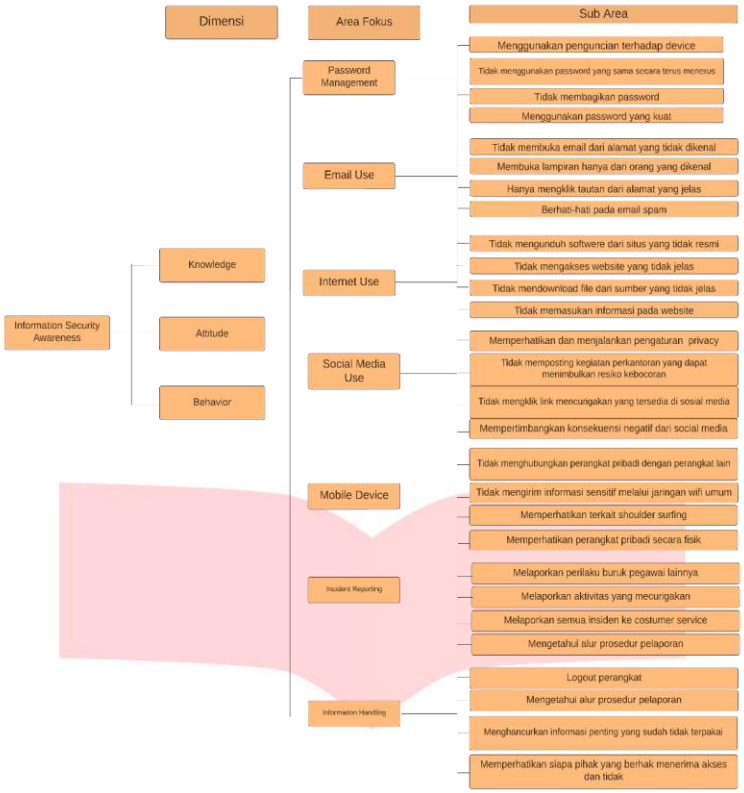


Gambar 2.1 Olahan Peneliti (2023)

2. Kerangka Pemikiran

Dengan mengadaptasi model kerangka pemikiran milik (Mahardika et al., 2020a) yang membuat kerangka pemikiran yang digunakan untuk mengukur kesadaran keamanan informasi pada penelitiannya untuk organisasi pemerintahan yang kemudian diadaptasi kembali oleh (Destya Atlanta et al., 2023) yang meneliti kesadaran keamanan dari pengguna aplikasi alodoc.

Berdasarkan penelitian-penelitian tersebut, peneliti mengadaptasi menyeluruh untuk dimensi dan focus area. Hal ini dilakukan dikarenakan HAIS-Q dirasa paling sesuai untuk digunakan dalam mengukur keamanan informasi dalam bidang MIGAS.



Gambar 2.1 Keranga Pemikiran

3. *Questionnaire Method*

Peneliti mempunyai total 84 pertanyaan dari kesadaran keamanan informasi untuk menguji *attitude, knowledge* serta *behavior* dalam perspektif pegawai Perusahaan X yang menggunakan perangkat digital sebagai sarana bekerja dan *environment* di perusahaan.

4. *Data Measurement*

Untuk dimensi *attitude* dan *knowledge* dijawab dengan skala 3 poin, yaitu setuju yang diberi nilai 3, tidak setuju memiliki nilai 1, dan tidak tahu memiliki nilai 2. Sedangkan untuk dimensi *behavior* hanya membutuhkan skala 2 poin, setuju dan tidak setuju. Kemudian, Setelah mendapatkan hasil dari perhitungan kuesioner, selanjutnya dilakukan analisis data menggunakan *Analytic Hierarchy Process (AHP)*. Hasilnya kemudian dikali dengan bobot pada fokus area dan dimensi yang ada. Bobot pada fokus area diasumsikan memiliki kepentingan yang sama atau setara sehingga bobotnya yaitu 1 dengan presentase (14,3%)

Dimensi	**Bobot**
Knowledge	30%
Attitude	20%
behavior	50%

Sumber: (Mahardika et al., 2020)

Kemudian, setelah dilakukan pembobotan, makan dapat dimasukan klasifikasi kategori. Hal ini dilakukan untuk mengetahui apakah hasilnya termasuk, baik, rata-rata, atau kurang.

Kriteria	Nilai	Keterangan
Good	77.7% - 100%	Tidak perlu dilakukan tindakan
Average	55.5% - 77.7%	Tindakan berpotensi dilakukan
Poor	33.3% - 55.5%	Dibutuhkan tindakan

Sumber: (Kencana Sari & Candiwan, 2014)

III. HASIL DAN PEMBAHASAN

A. Hasil Pengukuran

Hasil dari pengukuran tingkat kesadaran akan keamanan informasi akan dijelaskan sesuai dimensi masing-

masing. Pada bagian hasil akan dijelaskan item-item yang memiliki nilai tertinggi dan terendah dari tiap fokus area. Hal ini dilakukan dengan tujuan memberikan informasi terkait aspek-aspek yang lebih diperhatikan dan kurang diperhatikan oleh para pegawai divisi ICT perusahaan X

Tabel 3.1 Hasil pengukuran dimensi *knowledge*

Knowledge			
Fokus Area	**Item**	**Score**	**total**
Password Management	K1.1	89.6%	88.7%
	K1.2	85.2%	
	K1.3	94.0%	
	K1.4	85.8%	
Email Use	K2.1	93.4%	93.0%
	K2.2	91.3%	
	K2.3	91.3%	
	K2.4	96.2%	
Internet Use	K3.1	87.4%	89.6%
	K3.2	93.4%	
	K3.3	86.3%	
	K3.4	91.3%	
Social Media Use	K4.1	93.4%	90.6%
	K4.2	89.6%	
	K4.3	89.1%	
	K4.4	90.2%	
Mobile Device	K5.1	90.7%	89.8%
	K5.2	87.4%	
	K5.3	92.3%	
	K5.4	88.5%	
Incident Reporting	K6.1	88.5%	88.8%
	K6.2	87.4%	
	K6.3	88.5%	
	K6.4	90.7%	
Information Handling	K7.1	93.4%	91.8%
	K7.2	85.2%	
	K7.3	94.0%	
	K7.4	94.5%	

Tabel 3.1 menunjukan hasil dari dimensi knowledge. Dari tabel tersebut, dapat diketahui pada fokus area *password management* dari pegawai divisi ICT memiliki total nilai presentase sebesar 88.7% yang berarti masih masuk kategori baik atau *good* dengan nilai tertinggi dipegang oleh item K1.3 dengan pernyataan "Password hanya boleh diketahui oleh saya, tidak dibagikan kepada orang lain", dan item terendah dimiliki oleh item K1.2 dengan nilai 85.2% dengan pernyataan "Password sebaiknya diubah secara berkala". Untuk fokus area pada *email use* memiliki total nilai sebesar 93.0% yang berada dalam kategori baik, dengan nilai tertinggi dipegang oleh item K2.4 dengan pernyataan "Harus berhati-hati terhadap spam e-mail, agar terhindar dari penipuan yang dapat terjadi" dan terendah dipengang oleh K2.2 dan K2.3.

Untuk fokus area *internet use* memiliki total nilai rata-rata sebesar 89.1% yang menjadikan fokus area tersebut masih masuk kategori baik dengan item tertinggi dipegang oleh item K3.2 dengan pernyataan "Tidak mengakses situs website yang meragukan" dan terendah dimiliki oleh item "Mengunduh file dari sumber yang tidak jelas/terpercaya dapat berpotensi mengandung virus dan malware". Pada fokus area *social media use,* memiliki nilai sebesar 91.3% dengan item tertinggi pada K4.1 dengan pernyataan "Melakukan pengaturan security dan privacy pada akun social media agar keamanan data tetap terjaga" dan yang terendah dimiliki oleh item K4.3 dengan pernyataan "Melakukan klik link yang mencurigakan pada sosial media dapat menimbulkan ancaman".

Fokus area mobile device memiliki total nilai sebesar 89.8% dengan item tertinggi oleh K5.3 dengan pernyataan "Melaporkan semua insiden terkait kemanaan informasi kepada pihak yang bertanggung jawab" dan terendah dimiliki oleh K5.2 "Melaporkan semua aktivitas mencurigakan yang terjadi di perkantoran kepada user". Untuk fokus area *incident reporting,* memiliki total nilai sebesar 88.8% dengan item tertinggi dipegang oleh K6.4 dengan pernyataan "Menyimpan perangkat device (smartphone) dengan aman dapat membantu mencegahnya atau menghindari gangguan keamanan" dan yang terendah oleh item K6.2 dengan pernyataan "Pengiriman file atau data informasi menggunakan wifi umum dapat menimbulkan ancaman kemanan informasi saya", kemudian untuk fokus area yang terakhir dari dimensi *knowledge* memiliki nilai rata-rata sebesar 91.8% dengan item tertinggi dimiliki oleh item K7.4 dengan pernyataan "Memberikan informasi kepada orang yang berhak dan berwenang saja" dan item terendah dimiliki oleh item K7.2 dengan perntanyaan "Mengetahui alur dan cara pemberian informasi atau data penting dapat mengurangi kemungkinan adanya penyalahgunaan informasi".

Tabel 3.2 Hasil Pengukuran dimensi *attitude*

Attitude			
Fokus Area	Item	Score	total

ment	Password Manage-	A1.1	85.8%	88.8%
		A1.2	86.3%	
		A1.3	91.3%	
		A1.4	91.8%	
	Email Use	A2.1	86.3%	87.8%
		A2.2	89.1%	
		A2.3	87.4%	
		A2.4	88.5%	
	Internet Use	A3.1	87.4%	90.2%
		A3.2	91.3%	
		A3.3	94.0%	
		A3.4	88.0%	
	Social Media Use	A4.1	93.4%	91.4%
		A4.2	92.3%	
		A4.3	88.5%	
		A4.4	91.3%	
	Mobile Device	A5.1	90.7%	90.6%
		A5.2	90.7%	
		A5.3	92.9%	
		A5.4	88.0%	
	Incident Reporting	A6.1	92.9%	91.1%
		A6.2	88.5%	
		A6.3	86.3%	
		A6.4	96.7%	
dling	Information Han-	A7.1	97.3%	93.9%
		A7.2	91.3%	
		A7.3	92.3%	
		A7.4	94.5%	

Pada dimensi attitude ini, fokus area *password management* memiliki nilai sebesar 88.8% dengan nilai item tertinggi dimiliki oleh A1.4 denga pernyataan "Saya sadar bahwa dengan menggunakan password yang kuat dapat meningkatkan keamanan informasi" dan item terendah dimiliki oleh item A1.1 dengan pernyataan "Saya setuju bahwa penggunaan password/penguncian dapat membuat saya terhindar dari ancaman keamanan informasi". Untuk fokus area pada *email use* memiliki nilai total sebesar 87.8% dengan item tertinggi dimiliki oleh A2.2 dengan pernyataan *"*Saya sadar untuk menghindari ancaman keamanan sitem informasi, saya hanya membuka lampiran dari orang yang saya kenal saja", dan item terendah dimiliki oleh A2.1 dengan pernyataan "Saya sadar untuk tidak membuka lampiran e-mail dari alamat yang tidak saya kenal".

Fokus area *internet use* memiliki total nilai sebesar 90.2% dengan item tertinggi dimiliki oleh A3.3 dengan pernyataan "Saya sadar, mengunduh file dari sumber yang mencurigakan dapat menimbulkan ancaman keamanan informasi", dan item terendah pada A3.1 dengan pernyataan "Saya sadar untuk menghindari ancaman keamanan informasi, saya sebaiknya mengunduh software dari situs resmi". Untuk fokus area *social media use,* memiliki total nilai sebesar 91.4% dengan item tertinggi dimiliki oleh A4.1 dengan pernyataan "saya sadar untuk memperhatikan pengaturan privacy setting pada social media saya", dan item terendah dimiliki oleh A4.3 dengan pernyataan "Saya sadar untuk tidak sembarangan mengklik link yang ada di social media".

Fokus area *mobile device* memiliki total nilai sebesar 90.6% dengan item tertinggi dimiliki oleh item A5.3 dengan pernyataan "Saya setuju untuk melaporkan apabila telah terjadi insiden ke pihak yang bertanggung jawab" Dan item terendah dimiliki oleh A5.4 dengan pernyataan "Saya sadar untuk mengetahui prosedur alur pelaporan apabila adanya masalah pada keamanan informasi". Untuk fokus area *incident reporting* memiliki nilai rata-rata sebesar 91.1% dengan nilai item tertinggi dimiliki oleh A6.4 dengan pernyataan "Saya sadar untuk menyimpan perangkat saya secara aman", dan item terendah dimiliki oleh A6.3 dengan pernyataan "Saya sadar memperhatikan sekitar ketika memasukan informasi atau data sensitive, untuk terhindar dari *shoulder surfing".* Untuk fokus area yang terakhir dari dimensi attitude memiliki nilai rata-rata sebesar 93.9% dengan item tertinggi dimiliki oleh A7.4 dengan pernyataan "Saya sadar hanya memberikan akses kepada orang yang berhak dan mempunyai wewenang", dan item terendah dimiliki oleh A7.3 dengan pernyataan "Saya sadar untuk tidak membuang informasi yang bersifat sensitive secara sembarangan karena dapat menimbulkan resiko ancaman keamanan informasi".

Tabel 3.3 Hasil pengukuran dimensi *behavior*

Behavior			
Fokus Area	**Item**	**Score**	**total**
Password Management	B1.1	90.2%	85.8%
	B1.2	72.7%	
	B1.3	95.6%	
	B1.4	84.7%	
Email Use	B2.1	88.0%	88.5%
	B2.2	88.0%	
	B2.3	90.2%	

	B2.4	88.0%	
Internet Use	B3.1	84.7%	89.1%
	B3.2	83.6%	
	B3.3	93.4%	
	B3.4	94.5%	
Social Media Use	B4.1	93.4%	91.3%
	B4.2	86.9%	
	B4.3	94.5%	
	B4.4	90.2%	
Mobile Device	B5.1	88.0%	86.9%
	B5.2	83.6%	
	B5.3	90.2%	
	B5.4	85.8%	
Incident Reporting	B6.1	86.9%	88.0%
	B6.2	80.3%	
	B6.3	91.3%	
	B6.4	93.4%	
Information Handling	B7.1	91.3%	91.3%
	B7.2	85.8%	
	B7.3	98.9%	
	B7.4	89.1%	

Pada dimensi *behavior*, fokus area *password management* memiliki total nilai rata-rata sebesar 85.8% dengan nilai item paling besar pada B1.3 dengan pernyataan "Saya tidak pernah membagikan password saya ke orang lain", dan item paling kecil terdapat pada B1.2 dengan pernyataan "Saya selalu mengganti password saya secara berkala". Untuk fokus area email use, item terbesar dimiliki oleh B2.3 dengan pernyataan "Saya selalu berhati-hati terhadap email spam yang masuk". Untuk fokus area internet use, item terbesar dimiliki oleh B3.4 dan terendah pada B3.2, untuk fokus area social media use, item tertinggi dipegang oleh B4.3 dan terendah oleh B4.2, untuk fokus area mobile device, item tertinggi dimiliki oleh B5.3 dan terendah terendah oleh B5.2. Fokus area incident reporting tertinggi diperoleh item B6.4 dan information handling tertinggi oleh B7.1

No.		**Perusahaan X**			
		Dimensi			**Total**
		Knowledge	**Attitude**	**Behavior**	
	Fokus Area	30%	20%	50%	
1	Password Management	88.7%	88.8%	85.8%	87.3%
2	Email Use	93.0%	87.8%	88.5%	89.7%
3	Internet Use	89.6%	90.2%	89.1%	89.5%
4	Social Media Use	90.6%	91.4%	91.3%	91.1%
5	Incident Reporting	88.8%	91.1%	88.0%	88.9%
6	Mobile Devices	89.8%	90.6%	86.9%	88.5%
7	Information Handling	91.8%	93.9%	91.3%	91.9%
Total		90.3%	90.5%	88.7%	**89.5%**

Tabel diatas menunjukan total dari penelitian ini, dimensi knowledge memiliki nilai total dengan angka 90.3%, dimensi attitude memiliki nilai total dengan angka 90.5%, sedangkan dimensi behavior memiliki nilai total 88.7%. Untuk fokus area dengan presentase total terttinggi dimiliki oleh information handling dan presentase terendah dimiliki oleh password management. Kemudian, hasil dari total keseluruhan rata-rata dari pegawai divisi ICT perusahaan X menunjukan nilai sebesar 89.5% yang berarti masih masuk ke dalam kategori baik.

IV. KESIMPULAN DAN SARAN

A. Kesimpulan

Berdasarkan hasil keseluruhan, dimensi knowledge memiliki total angka 90.3%, dan dimensi attitude memiliki hasil total sebesar 90.5%, dan dimensi behavior memiliki hasil keseluruhan 88.7% hasil dari tiap dimensi menunjukukan kriteria yang masuk kedalam kategori baik atau tidak diperlukannya Tindakan. Kemudian, untuk total secara keseluruhan dari pengukuran penelitian menunjukan angka adalah 89.5%. Dengan demikian dapat disimpulkan bahwa kesadaran keamanan dari pegawai perusahaan X sudah masuk ke dalam kategori baik atau *good.* Dengan begitu, pegawai divisi ICT perusahaan X terbukti sudah sadar akan pentingnya keamanan informasi dari sisi pengetahuan, sikap, dan perilaku.

B. Saran

1. Saran Teoritis

Penulis berharap dapat memberikan pengetahuan atau wawasan mengenai pentingnya kesadaran keamanan informasi khususnya pada bagian pegawai perusahaan MIGAS. Perusahaan yang bukan bergerak di bidang teknologi namun tetap harus memperhatikan aspek keamanan informasinya, karena ancaman keamanan informasi bagi perusahaan pegawainya jika tidak diperhatikan kesadarannya. penulis harap penelitian ini akan dapat digunakan untuk penelitian selanjutnya.

2. Saran Praktis

Hasil dari penelitian ini menghasilkan kesimpulan bahwa kesadaran keamanan informasi dari pegawai divisi ICT perusahaan minyak X adalah baik atau "*good"*. Hal ini membuktikan bahwa pegawai sudah menyadari pentingnya keamanan informasi. hal ini dapat dioptimalkan kembali dengan melakukan perkembangan dan perbaikan pada fokus area yang memiliki nilai terendah. Nilai terendah dari total keseluruhan ada pada *password management* dengan angka 87.3%, memang angka tersebut masih masuk kedalam kriteria *good* karena berada pada kisaran 77,78-100. Namun masi dapat ditingkatkan dengan cara pemberian seminar atau sosialisasi mengenai hal teresut.

REFERENSI

Destya Atlanta, N. S., Candiwan, C., Sari, P. K., & Omar Sharif, O. (2023). *Information Security Awareness Evaluation of Telemedicine Application Users using Human Aspect Information System Questionnaire*. 1–6. https://doi.org/10.1109/icced56140.2022.10010445

Kencana Sari, P., & Candiwan. (2014). Measuring information security awareness of Indonesian smartphone users. *Telkomnika (Telecommunication Computing Electronics and Control)*, *12*(2), 493–500. https://doi.org/10.12928/TELKOMNIKA.v12i2.2015

Mahardika, M. S., Hidayanto, A. N., Paramartha, P. A., Ompusunggu, L. D., Mahdalina, R., & 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), 501–509. https://doi.org/10.25046/aj050362

Makkasau, K. (2012). Use of Analytic Hierarchy Process (Ahp) Methods in Determining the Priority of Health Programs (Case Study of Health Promotion Program). *J@TI Undip*, *VII*(2), 105–112. https://doi.org/USE OF ANALYTIC HIERARCHY PROCESS (AHP) METHODS IN DETERMINING THE PRIORITY OF HEALTH PROGRAMS (CASE STUDY OF HEALTH PROMOTION PROGRAM)

Munthe, I. R., & Purnama, I. (2019). Uji Tingkat Kesadaran Keamanan Informasi Pengguna Smartphone (Studi Kasus: Amik Labuhan Batu). Jurnal Teknik Informasi Dan Komputer (Tekinkom), 2(2), 156. https://doi.org/10.37600/tekinkom.v2i2.113

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers & Security*, *66*, 40–51. https://doi.org/10.1016/J.COSE.2017.01.004

Singgalen, Y. A., Purnomo, H. D., & Sembiring, I. (2021). Exploring MSMEs Cybersecurity Awareness and Risk Management: Information Security Awareness. *IJCCS (Indonesian Journal of Computing and Cybernetics Systems)*, *15*(3), 1–12.