Faktor Manajemen Keamanan Informasi Terhadap Perilaku Keamanan Siber Pegawai di Sektor Pemerintah

Komang Anugrah Mas Dana Putra[1], Candiwan Candiwan[2]
[1] Manajemen Bisnis Telekomunikasi & Informatika, Fakultas Ekonomi dan Bisnis, Universitas Telkom, Indonesia, mangdana@student.telkomuniversity.ac.id
[2] Manajemen Bisnis Telekomunikasi & Informatika, Fakultas Ekonomi dan Bisnis, Universitas Telkom, Indonesia, candiwan@telkomuniversity.ac.id

Abstrak

Perkembangan Perkembangan digitalisasi telah mendorong sektor pemerintahan untuk mengadopsi teknologi informasi dalam berbagai proses kerja dan pelayanan publik. Namun, pemanfaatan teknologi tersebut juga memunculkan tantangan baru berupa ancaman keamanan siber. Beberapa kasus peretasan instansi pemerintah menunjukkan masih rendahnya kesadaran akan pentingnya keamanan informasi di kalangan pegawai. Hal ini berdampak negatif pada kepercayaan publik serta mengancam keamanan data strategis negara. Penelitian ini bertujuan untuk menganalisis pengaruh manajemen keamanan informasi terhadap perilaku keamanan siber pegawai pemerintah. Fokus penelitian mencakup beberapa faktor, yaitu pengelolaan infrastruktur, kebijakan organisasi, dukungan dan pelatihan, manajemen kata sandi, manajemen email, dan persepsi keamanan. Objek penelitian adalah pegawai Pemerintah Kota Bandung yang bekerja di Dinas Komunikasi dan Informatika serta Dinas Kependudukan, Pencatatan Sipil dan Kepegawaian Pengembangan Sumber Daya Manusia.

Penelitian ini menggunakan pendekatan kuantitatif dengan metode survei. Data dikumpulkan melalui kuesioner dan dianalisis menggunakan teknik *Partial Least Squares Structural Equation Modeling* (PLS-SEM) yang mampu menguji hubungan antar variabel secara menyeluruh dan memberikan hasil yang relevan dengan tujuan penelitian. Hasil penelitian menunjukkan bahwa sebagian besar variabel memiliki pengaruh signifikan terhadap perilaku keamanan siber pegawai. Tiga faktor utama yang terbukti mendorong perilaku keamanan yang lebih baik adalah *Infrastructure Security Management, Password Management, dan Email Management*.

Penelitian ini memberikan kontribusi praktis bagi instansi pemerintah dalam membentuk strategi peningkatan kesadaran keamanan informasi. Disarankan agar instansi memperkuat pengelolaan infrastruktur, meningkatkan edukasi terkait pengelolaan kata sandi, serta memberikan pelatihan rutin untuk mencegah ancaman *email* seperti *phishing*. Penelitian selanjutnya dapat dilakukan di instansi berbeda dengan jumlah responden yang lebih luas guna memperoleh hasil yang lebih general.

Kata Kunci-Keamanan siber, Kesadaran Keamanan informasi, Kebocoran Data, Pemerintah, Ancaman Siber, Manajemen Keamanan Informasi.

I. PENDAHULUAN

digitalisasi memungkinkan terjadinya otomatitasi pada semua bidang yang menyatukan fisik dengan digital yang akan mengubah pola interkasi pada manusia (Intan & Yasin, 2024).Teknologi sekarang menjadi bagian penting dalam banyak bidang kehidupan, memberikan pengaruh besar pada perubahan-perubahan yang mendasar (Suryadi, 2019). Seiring dengan meningkatnya digitalisasi mencakup aspek kehidupan sehari-hari yang memungkinkan terjadinya tantangan yang baru terutama dalam aspek keamanan siber.

Cybersecurity adalah salah satu masalah keamanan yang paling menantang saat ini bagi perusahaan komersial, lembaga pemerintah, serta individu (Andriessen et al., 2022). Kesadaran keamanan siber dapat diartikan sebagai tingkat pemahaman atau pengetahuan mengenai keamanan siber, hal ini mencakup kesadaran akan berbagai risiko dan ancaman siber serta pemahaman mengenai langkah-langkah perlindungan yang tepat (Nurse, 2021). Menurut (Azizi et al., 2024) Menjelaskan bahwa Keamanan siber juga dapat diartikan sebagai usaha untuk melindungi dari berbagai serangan di dunia maya, penerapannya tidak hanya berfokus pada perangkat tetapi juga perlu membangun pemahaman mengenai kesadaran keamanan pada sumber daya manusia. *Association of Computing Machinery* (ACM) menjelaskan terdapat beberapa kategori yang menjelaskan bagian dari keamanan siber yaitu *Data security* (Keamanan Data) yang mengacu pada perlindungan data digital, Software Security (Keamanan Perangkat lunak) pelindungan terhadap sistem yang rawan akan kerentanan, *Connection Security* (Keamanan Koneksi) pelindungan yang timbul saat terhubung dengan perangkat atau jaringan yang terhubung, *System Security* (Keamanan sistem) Keamanan dalam sistem secara keseluruhan dengan beberapa komponen yang berbeda, *Human Security* (Keamanan manusia) perlindungan terhadap manusia yang berkaitan dengan infromasi individu ataupun dengan organisasi, *Organizational Security* (Keamanan Organisasi) melindungi infrastuktur dari ancaman internal maupun eksternal dan *Social Security* (Keamanan sosial) berfokus kepada kejahatan dunia maya, etika dan hukum yang menyangkut Masyarakat.

Menurut Data (BSSN, 2023) telah menerima aduan sebanyak 1.417 aduan dari berbagai kategori pengaduan terbanyak cybercrime dengan jumlah sebanyak 86% aduan, jenis kasus yang paling banyak terjadi ialah Web defacement, Ransomeware dan Data Branch. Rekapitulasi oleh tim pusat kontak siber BSSN mencatat 186 insiden Sektor yang paling banyak mengalami insiden adalah Pemerintah, yaitu sebesar 69%. Selain itu, kasus yang paling terbaru yang menyerang sektor pemeritah terjadi pada 20 Juni 2024 yaitu serangan siber terhadap Pusat Data Nasional (PDN), yang mengakibatkan kebocoran data dan membuat 282 layanan dari berbagai instansi pemerintah. Setelah perangkat terinfeksi ransomware, pelaku utama yang merupakan hacker menyandera data penting negara dan menuntut tebusan sebesar 8 juta dolar Amerika (sekitar 131 miliar rupiah) untuk mengembalikan akses ke data yang telah dicuri (Anto, 2024). Situasi ini diakibatkan oleh kelalaian oknum seperti merenspons notifiikasi dan kurangnya kesadaran individu terhadap kesadaran keamanan siber pada instansi terkait data negara. Penggunaan teknologi yang tidak bijak ditambah dengan kurangnya kesadaran dapat meningkatkan risiko terjadinya kejahatan di dunia siber (Candiwan et al., 2022).

Kasus Serupa juga Sempat terjadi peretasan di website resmi Pemkot Bandung (bandung.go.id) Situs resmi Pemkot Bandung mengunggah konten yang memuat nama partai politik di Pemilu 2024 (Diskominfo Bandung, n.d.) sehingga hal tersebut dapat mengakibatkan kehilangan kepercayaan publik, karena masyarakat menganggap situs pemerintah sebagai sumber informasi yang harusnya aman dan terpercaya. Selain itu, peretasan ini bisa mencemari netralitas pemerintah, karena munculnya konten politik yang tidak seharusnya ada di situs resmi. Jika data sensitif berhasil diakses, hal ini berpotensi menimbulkan penyalahgunaan data pribadi warga. Pemerintah kota Bandung juga bisa menghadapi kerugian finansial akibat biaya pemulihan dan dampak reputasi yang tercemar. Tidak hanya itu, peretasan ini dapat berpotensi terhadap serangan lanjutan pada sistem atau situs lain yang lebih berisiko. sangat penting bagi Pegawai pemerintah dalam memahami kesadaran keamanan siber dalam upaya pencegahan kebocoran data yang terkait dengan information security behaviour.

Dilansir dari situs (Maheswara, 2023) Terdapat sekitar 1 miliar anomali lalu lintas yang menunjukkan adanya aktivitas malware. Menurut (Saeed, 2023a) *Infrastructure Management, Organizational Policy, Organizational Support & Training, Password Management, Email Management perception security* adalah faktor yang berpengaruh terhadap peningkatan perilaku positif seseorang terhadap keamanan siber. Menurut (Grassegger & Nedbal, 2021) yang berjudul *The role of employees' information security awareness on the intention to resist social engineering*, Hasil dari penelitian tersebut ialah menunjukkan bahwa kecenderungan perilaku berisiko memengaruhi kesadaran keamanan siber karyawan. Hal tersebut juga dijelaskan oleh (Alghazo et al., 2023) dan (Rocha Flores & Ekstedt, 2016) Menyoroti bahwa pemimpin keamanan dengan

kompetensi keamanan siber yang memadai secara positif mempengaruhi kesadaran karyawan tentang penanggulangan keamanan Siber.

Dapat disimpulkan Peneliti berasumsi bahwa Perilaku keamanan siber *Infrastructure Management, Organizational Policy, Organizational Support & Training, Password Management, Email Management and* . Fokus dalam penelitian ini adalah human security yaitu memahami perilaku praktik keamanan siber pada pegawai pemerintah, tujuan dari penelitian dapat meningkatkan kesadaran keamanan pegawai serta untuk membekali mereka dengan lebih baik untuk menghadapi tantangan keamanan siber, serta untuk melindungi sumber daya organisasi Penelitian ini dilaksanakan dengan objek pegawai pada sektor Pemerintah Kota Bandung, khususnya instansi yang memiliki tugas pokok dan fungsi (tupoksi) yang berkaitan erat dengan pemanfaatan teknologi informasi dalam memberikan layanan publik serta mengelola data masyarakat (Priyatna, 2022)

II. TINJAUAN LITERATUR

A. Manajemen

Manajemen adalah sebuah proses yang melibatkan pemahaman mendalam terhadap berbagai situasi yang dihadapi oleh organisasi atau individu. Proses ini mencakup langkah-langkah dalam menganalisis kondisi yang ada, mengambil keputusan yang tepat, dan menyusun rencana tindakan yang dirancang khusus untuk menyelesaikan masalah atau mencapai tujuan yang telah ditetapkan. Manajemen mengidentifikasi tantangan dalam lingkungan, menyusun strategi organisasi untuk mengatasinya, serta mengelola sumber daya manusia dan finansial guna mengoordinasikan aktivitas dan mencapai keberhasilan (Laudon, Kenneth C., 2016). Manajemen dan sistem siber merupakan dua elemen yang saling berkaitan dalam mendukung keberhasilan organisasi. Sistem Manajemen adalah kumpulan komponen yang bekerja saling terhubung untuk mengumpulkan, memproses, menyimpan, dan mendistribusikan data untuk mendukung pengambilan keputusan dan kontrol dalam suatu organisasi (Laudon, Kenneth C., 2016).

B. Kesadaran Keamanan Informasi

Keamanan siber merupakan aspek utama dalam melindungi aset organisasi, termasuk dokumen, data, perangkat keras dan lunak, serta infrastruktur pendukung yang menjadi fondasi operasional. Keamanan siber mencakup upaya perlindungan terhadap seluruh sumber daya agar tidak disalahgunakan oleh pihak yang tidak berwenang, serta langkah strategis untuk menjamin kelangsungan operasional organisasi (Ciekanowski et al., 2024). Dalam konteks ini, privasi menjadi elemen penting yang mencakup hak dasar individu, nilai berharga yang rentan terhadap serangan, kondisi pembatasan akses data pribadi, serta kemampuan individu dalam mengontrol informasi pribadinya secara digital (Ernita et al., 2022). Untuk menjaga keamanan siber, perlu ada pengelompokan komponen inti yang saling mendukung seperti *physical security* (perlindungan aset fisik dan manusia), *personal security* (perlindungan individu), *identification* (pengenalan pengguna), *authentication* (verifikasi identitas), dan *network security* (perlindungan jaringan dan data) (Yel & Nasution, 2022). Penerapan regulasi dan framework keamanan siber memungkinkan organisasi mengidentifikasi celah keamanan, mengalokasikan sumber daya secara efektif, serta memitigasi risiko dari ancaman eksternal seperti ransomware maupun dari dalam organisasi akibat kelalaian karyawan, dengan implementasi kepatuhan yang konsisten sebagai kunci utama pencegahan.

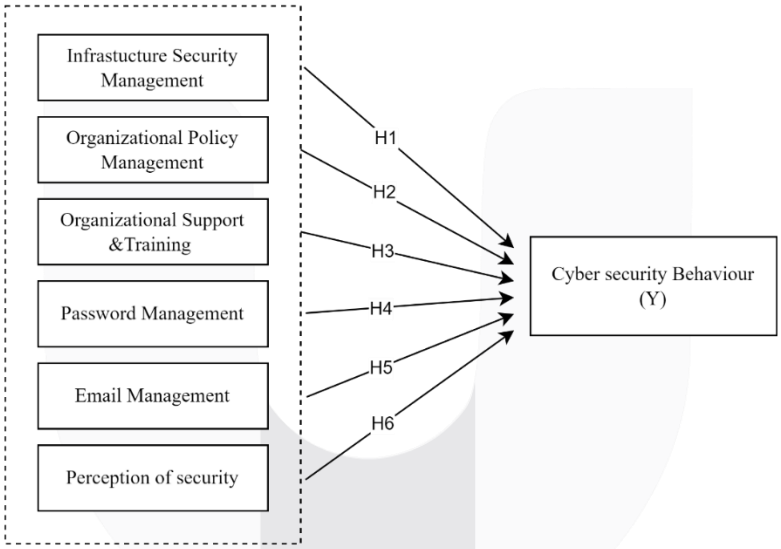
C.

Dalam penelitan sebelumnya banyak yang membahas terkait dengan perilaku kesadaran keamanan siber. Penelitian yang dilakukan oleh (Saeed, 2023a), dalam jurnal yang berjudul membahas terkait faktor yang relevan terkait dengan infrastuktur digital pada lingkungan kerja digital yang berkaitan dengan Perilaku Keamanan siber serta menyatakan beberapa faktor tidak relevan sehingga perlu ditingkatkan. Kemudian (Saeed, 2023b) juga menjelaskan dalam membahas mengenai dengan perilaku keamanan infromasi pada sektor Pendidikan, yang menyatakan beberapa elemen tidak relevan terkait dengan Perilaku Keamanan siber. Selanjutnya penelitian yang dilakukan oleh (Fadlika et al., 2023) dalam penelitianya yang berjudul

menjelaskan terkait dengan perilaku keamanan infromasi pada karyawan yang menggunakan metode HAIS-Q model, dengan hasilnya yaitu bahwa pengetahuan, sikap dan perilaku saling terintegrasi sehingga menimbulkan Perilaku kesadaran Keamanan yang positif, Dan penelitan yang dilakukan oleh (Yassen, 2023). Dengan penelitianya yang berjudul menjelaskan Faktor manusia telah terbukti menjadi yang paling penting dalam keamanan siber sehingga perilaku yang positif akan berkontribusi dalam perlindungan keamanan pada individu ataupun organisasi. Selanjutnya penelitian yang dilakukan oleh (Candiwan et al., 2022) dalam jurnal yang berjudul "*Analysis of Behavioral and Information Security Awareness among Users of Zoom Application in COVID-19 Era; International Journal of Safety and Security Engineering*" bahwa hasil dalam penelitian tersebut menunjukkan bahwa terdapat perbedaan yang signifikan antara variabel demografi dan pendekatan.

Kemudian penelitian (Ciekanowski et al., 2024) dalam jurnalanya yang berjudul yang menjelaskan bahwa. Organisasi yang tidak mengambil tindakan di bidang keamanan siber tidak hanya berisiko mengalami kerugian finansial atau kehilangan reputasi, tetapi juga kemungkinan terhentinya operasi selanjutanya. Menurut (Grassegger & Nedbal, 2021)Hasil dari penelitian tersebut ialah menunjukkan bahwa dan kecenderungan perilaku berisiko memengaruhi kesadaran keamanan siber karyawan. Hal tersebut juga dijelaskan oleh (Alghazo et al., 2023) dan (Rocha Flores & Ekstedt, 2016) Menyoroti bahwa pemimpin keamanan dengan kompetensi keamanan siber yang memadai secara positif mempengaruhi kesadaran karyawan tentang penanggulangan keamanan Siber.

Berdasarkan teori diatas dapat dibentuk kerangka berpikir dan hipotesis sebagai berikut:



Gambar 1. Kerangka Pemikiran (Sumber: Data Olahan Peneliti)

H1 : Penerapan perangkat lunak yang tepat mengarah pada prilaku keamanan siber yang positif pada organisasi pemerintah.
H2 : Kebijakan keamanan organisasi mengarah pada perilaku keamanan siber yang positif.
H3 : Dukungan dan pelatihan yang memadai mengarah pada positif prilaku yang Positif.
H4 : Pengelolaan kata sandi yang tepat mengarah pada perilaku keamanan siber yang positif,
H5 : Praktik manajemen email yang tepat mengarah pada perilaku yang positif dalam keamanan siber.
H6 : Persepsi keamanan berdampak pada perilaku keamanan siber yang positif

III. METODOLOGI PENELITIAN

A. Instrumen Penelitian dan Pengumpulan Data

Tujuan Penelitian tersebut ialah kausal untuk mengetahui sebab akibat mengetahui hubungan antara variabel independent dan dependen. Menurut (Sekaran & Bougie, 2016) Penelitian kausal bertujuan untuk mengidentifikasi sifat hubungan antara variabel-variabel yang diteliti, serta memahami dampak dari satu variabel terhadap variabel lainnya dalam rangka menjelaskan fenomena. Bedasarkan Latar belakang, Perumusan masalah dan Kerangka pemikiran yang telah di susun maka penelitan akan menggunakan metode kuantitatif karena teknik tersebut akan menghasilkan temuan melalui penggunan teknik statistik dari proses pengukuran. Kemudian Bedasarkan metode penelitian tersebut strategi yang digunakan dalam penelitian tersebut ialah survei dengan penyebaran kuisioner yang sudah di validasi kemudian di distribusikan kepada responden objek penelitian. Karakteistik unit analisis dalam penelitian ini ialah unit analisis tingat inidividu, dikarenkan mengetahui bagaimana perilaku keamanan siber. Unit analisis individu berarti data diperoleh dari setiap orang secara langsung, di mana setiap individu memberikan respons yang menjadi sumber data utama. (Sekaran & Bougie, 2016)

Pada penelitian ini peneliti tidak terlalu campur tangan terhadap data penelitian sehinggan tergolong keterlibatan minimal. Selanjutnya latar penelitian yang dilakukan bersifat non-contrived setting, yaitu lingkungan dengan fenomena yang alami tanpa keterlibatan peneliti (Sekaran & Bougie, 2016)Pelaksanaan penelitian dengan desain cross-sectional dilakukan dengan mengumpulkan data hanya satu kali, yang dapat berlangsung dalam rentang waktu beberapa hari, minggu, atau bulan.

Instrumen penelitian terdiri dari kuesioner yang menggunakan skala Likert lima poin untuk mengukur tingkat kesetujuan responden terhadap pernyataan yang berkaitan dengan keamanan siber. Validitas instrumen diuji dengan menggunakan uji validitas konvergen dan diskriminan, sedangkan reliabilitas dinilai dengan menggunakan metode Cronbach's Alpha, seperti yang disajikan dalam Tabel 1

Tabel 1. Sekala Likert

Skor	Keterangan
5	Sangat Baik/Sangat Setuju
4	Baik/Setuju
3	Netral
2	Tidak Baik/Tidak Setuju
1	Sangat Tidak Setuju

Sumber : Data Olahan Peneliti (2025)

B. Teknik Analisis

Penelitian ini menggunakan data primer dan sekunder. Data primer dikumpulkan melalui kuesioner yang terdiri dari 35 pertanyaan, yang didistribusikan melalui Google Forms. Penyebaran kuesioner difasilitasi oleh kepala survei dari kedua lembaga terkait, dengan jangka waktu pengembalian kuesioner selama dua minggu setelah penyebaran. Sementara itu, data sekunder diperoleh dari laporan tahunan pemerintah, yang memberikan informasi mengenai jumlah pegawai pada tahun terakhir.

Metode pengambilan sampel dalam penelitian ini menerapkan probability sampling dengan menggunakan teknik simple random sampling, dimana setiap anggota populasi memiliki probabilitas yang sama untuk terpilih. Pendekatan ini memastikan bahwa sampel yang terpilih secara objektif mewakili populasi dan meminimalisir potensi bias dalam pemilihan responden. Untuk menentukan jumlah sampel minimum yang representatif, penelitian ini menggunakan rumus Slovin, yang memungkinkan peneliti untuk menghitung jumlah sampel yang diperlukan dan margin of error sesuai kebutuhan. Rincian lebih lanjut mengenai metode ini disajikan dalam Rumus 3.1

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

dimana:

n = Sampel yang dicari

N = Jumlah populasi

e = nilai margin of error (besar kesalahan dari jumlah populasi)

IV. HASIL DAN PEMBAHASAN

A. Analisis Deskriptif

Menyajikan karakteristik responden, memberikan data demografis dari para partisipan yang terlibat dalam penelitian ini. Data tersebut mencakup lima aspek utama: jenis kelamin, jabatan, masa kerja, generasi berdasarkan tahun kelahiran, dan latar belakang pendidikan terakhir. Informasi ini bertujuan untuk memberikan gambaran umum mengenai profil responden, sehingga memudahkan pemahaman yang lebih baik mengenai latar belakang individu yang berkontribusi terhadap temuan studi.

Tabel 2. Karaktersistik Responden

Characteristics		Count	Percentage
Gender	Male	112	57,7%
	Female	82	42,3 %
Position	OP	109	56,1%
	FO	79	40,7 %
	S0	6	4,0 %
Length of Service	<1 Years	97	50,0%
	1–3 Years	38	28,3%
	4–6 Years	42	17,5%
	>6 Years	15	5,0%
Generation	Boomer	3	1,5%
	Gen X	50	25,7%
	Gen Millennial	101	52,0%
	Gen Z	40	20,61%
Education	D3	30	15,4%
	D4	29	14,9%
	S1	85	43,8%
	S2	30	15,4%

Sumber : Data Olahan Peneliti (2025)

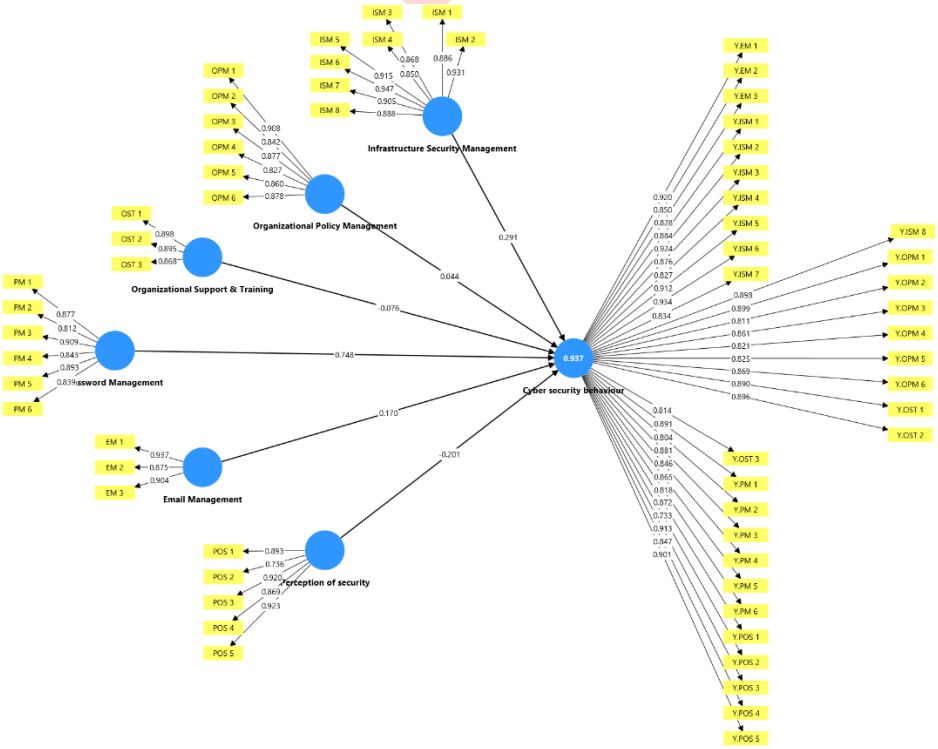
Tabel 3 menyajikan ringkasan hasil analisis deskriptif terhadap tujuh variabel utama yang diteliti, yaitu *Infrastructure Security Management, Organizational Policy Management, Organizational Support and Training, Password Management, Email Management, Perception of Security*. Seluruh variabel menunjukkan tingkat persentase skor antara 63,60% hingga 67,42%, yang diklasifikasikan dalam kategori “cukup baik”. Variabel dengan persentase tertinggi adalah Infrastructure Security Management (67,42%), sedangkan yang terendah adalah Perception of Security (63,60%). Meskipun demikian, pada masing-masing variabel terdapat indikator yang menonjol dengan nilai tertinggi, seperti ISM 2, OPM 2, dan OST 2, yang dapat menjadi acuan dalam penguatan aspek lainnya. Secara umum, temuan ini mengindikasikan bahwa penerapan keamanan informasi dalam organisasi sudah cukup baik namun masih memerlukan peningkatan agar mencapai kategori baik secara menyeluruh.

Tabel 3. Analaisis Deskriptif

Variabel	Total Skor	Skor Ideal	Persentase	Klasifikasi	Item Terendah
Infrastructure Security Management (ISM)	5.232	7.760	67,42%	Cukup Baik	ISM 3, ISM 4 ISM 8
Organizational Policy Management (OPM)	3.789	5.820	65,10%	Cukup Baik	OPM 1, OPM 3, OPM 4 OPM 5
Organizational Support and Training (OST)	1.996	2.910	68,77%	Cukup Baik	OST 1, OST 3
Password Management (PM)	3.720	5.820	63,91%	Cukup Baik	PM 1, PM 2, PM 3, PM 5, PM 6
Email Management (EM)	1.936	2.910	66,52%	Cukup Baik	EM 2, EM 4
Perception of Security (POS)	3.083	4.850	63,60%	Cukup Baik	POS 1 – POS 5

Sumber : Data Olahan Peneliti (2025)

B. Analisis Multivariant



Gambar 2. Outer Model

Hasil penilaian Outer Model yang ditampilkan pada Gambar 2 menunjukkan bahwa seluruh indikator dalam penelitian ini memiliki validitas dan reliabilitas yang kuat. Hal ini dibuktikan dengan nilai loading factor yang sebagian besar berada di atas ambang batas 0,7, yang mengindikasikan bahwa setiap indikator memberikan kontribusi yang signifikan dalam menjelaskan variabel laten yang bersangkutan. Selain itu, nilai RHO_A, RHO_C, dan *Cronbach's Alpha* juga semuanya melampaui nilai ambang 0,7, yang mencerminkan tingkat konsistensi internal yang tinggi serta mengonfirmasi bahwa instrumen penelitian yang digunakan sudah reliabel untuk analisis lebih lanjut. Secara

keseluruhan, temuan ini menunjukkan bahwa instrumen penelitian yang digunakan dalam skripsi ini telah memenuhi kriteria validitas dan reliabilitas yang ditetapkan.

Hasil pengujian cross-loading yang disajikan pada Tabel 3 menunjukkan bahwa setiap indikator memiliki korelasi yang lebih tinggi terhadap konstruk laten yang diukur dibandingkan dengan konstruk lainnya dalam model. Hal ini mengonfirmasi bahwa instrumen penelitian memenuhi syarat validitas diskriminan, di mana setiap indikator lebih efektif dalam menjelaskan variabel yang dimaksud dibandingkan variabel lain yang tidak relevan. Sebagai contoh, indikator ISM6 menunjukkan nilai loading tertinggi pada *konstruk Infrastructure Security Management* (0,944), yang memperkuat bahwa indikator tersebut merepresentasikan konstruk yang dimaksud secara akurat. Pola serupa juga ditemukan pada variabel lainnya seperti *Organizational Policy Management, Organizational Support & Training, Password Management, Email Management, Perception of Security, dan Leadership*, di mana setiap indikator menunjukkan loading tertinggi pada konstruk yang sesuai. Hasil ini semakin memperkuat validitas instrumen penelitian dan menunjukkan bahwa model yang digunakan dalam studi ini relevan dan dapat diandalkan dalam menganalisis faktor-faktor yang memengaruhi perilaku keamanan siber di kalangan pegawai pemerintah.

Tabel 4. Cross Loading

Indicator	Email Management	Infrastructure Security Management	Organizational Policy Management	Organizational Support & Training	Password Management	Perception Of Security
EM1	0.937	0.895	0.921	0.918	0.921	0.918
EM2	0.875	0.833	0.854	0.847	0.850	0.867
EM3	0.904	0.841	0.804	0.809	0.791	0.817
ISM1	0.842	0.791	0.886	0.847	0.835	0.853
ISM2	0.905	0.909	0.931	0.906	0.912	0.922
ISM3	0.848	0.873	0.868	0.883	0.856	0.870
ISM4	0.802	0.735	0.850	0.851	0.812	0.841
ISM5	0.885	0.894	0.915	0.919	0.920	0.906
ISM6	0.909	0.912	0.947	0.929	0.940	0.926
ISM7	0.839	0.819	0.905	0.850	0.844	0.847
ISM8	0.864	0.863	0.888	0.893	0.914	0.912
OPM1	0.866	0.800	0.916	0.908	0.891	0.900
OPM2	0.811	0.878	0.807	0.842	0.799	0.822
OPM3	0.851	0.884	0.866	0.877	0.874	0.884
OPM4	0.798	0.774	0.832	0.827	0.843	0.830
OPM5	0.803	0.737	0.837	0.860	0.823	0.840
OPM6	0.842	0.862	0.852	0.878	0.848	0.855
OST1	0.868	0.925	0.860	0.870	0.898	0.885
OST2	0.869	0.833	0.923	0.895	0.895	0.886
OST3	0.799	0.764	0.820	0.838	0.868	0.857
PM1	0.871	0.887	0.895	0.867	0.887	0.877
PM2	0.793	0.785	0.817	0.824	0.808	0.812
PM3	0.856	0.803	0.872	0.870	0.882	0.909
PM4	0.831	0.836	0.851	0.827	0.821	0.843
PM5	0.846	0.850	0.839	0.886	0.887	0.893
PM6	0.795	0.725	0.819	0.843	0.822	0.839
POS1	0.857	0.856	0.884	0.884	0.875	0.880
POS2	0.703	0.650	0.727	0.757	0.741	0.739
POS3	0.883	0.878	0.931	0.906	0.899	0.901
POS4	0.824	0.895	0.829	0.851	0.840	0.838
POS5	0.886	0.877	0.907	0.918	0.930	0.931

Sumber : Data Olahan Peneliti (2025)

Hasil pengujian *Fornell-Larcker* yang ditampilkan pada Tabel 5 menunjukkan bahwa nilai akar kuadrat dari *Average Variance Extracted (AVE*) untuk setiap konstruk lebih tinggi dibandingkan dengan korelasi konstruk tersebut terhadap konstruk lainnya dalam model. Hal ini mengonfirmasi bahwa instrumen pengukuran memenuhi validitas diskriminan, yang berarti bahwa masing-masing variabel mampu menjelaskan varians indikator-indikatornya secara lebih kuat daripada korelasinya dengan variabel lain. Sebagai contoh, menunjukkan korelasi tertinggi terhadap dirinya sendiri dibandingkan dengan variabel lain seperti Email Management (0,937) Pola yang sama juga terlihat pada

konstruk lainnya seperti, *Organizational Policy Management, Organizational Support & Training, Password Management, dan Perception of Security,* di mana nilai tertinggi berada pada bagian diagonal dari matriks dibandingkan dengan nilai korelasi antar konstruk

Tabel 5. Fornell Lacker

Indicator	Email Management	Infrastructure Security Management	Orgainazational Policy Management	Organizational Support & Training	Password Management	Perception Of Security
EM	0.959					
ISM	0.947	0.986				
OPM	0.951	0.985	0.993			
OST	0.949	0.979	0.979	0.987		
PM	0.945	0.984	0.989	0.887	0.988	
POS	0.906	0.899	0.866	0.987	0.863	0.871

Sumber : Data Olahan Peneliti (2025

Tabel 6 menunjukkan bahwa sebesar 93,5% variasi dalam Perilaku Keamanan Siber dapat dijelaskan oleh variabel-variabel independen yang terdapat dalam model, sementara sisanya sebesar 6,1% dipengaruhi oleh faktor-faktor di luar model. Nilai Adjusted R-Square sebesar 0,935 semakin menguatkan bahwa model ini memiliki kemampuan prediktif yang tinggi. Temuan ini mengindikasikan bahwa variabel-variabel seperti Manajemen Keamanan Infrastruktur Manajemen Kebijakan Organisasi, Dukungan dan Pelatihan Organisasi, Manajemen Kata Sandi, Manajemen Email, serta Persepsi terhadap Keamanan, memiliki pengaruh yang signifikan terhadap perilaku keamanan siber para pegawai. Dengan demikian, hasil ini mendukung validitas dan kekuatan penjelasan dari model yang digunakan dalam penelitian ini.

Tabel 6. R-Sequare

Variable	R-square	R-square adjusted
Cyber Security Behaviour	0.937	0.935

Sumber : Data Olahan Peneliti (2025)

Hasil uji F-Square yang ditampilkan dalam Tabel 7 menunjukkan bahwa variabel Manajemen Kata Sandi memiliki pengaruh paling signifikan terhadap Perilaku Keamanan Siber, dengan nilai F-Square sebesar 0,109. Nilai ini mencerminkan kontribusi yang cukup kuat terhadap model. Sementara itu, variabel Manajemen Keamanan Infrastruktur (0,031) dan Manajemen Email (0,036) memberikan pengaruh yang relatif kecil namun tetap bermakna terhadap perilaku keamanan siber pegawai pemerintah. Di sisi lain, variabel Dukungan dan Pelatihan Organisasi (0,003) serta Persepsi terhadap Keamanan (0,005) menunjukkan pengaruh yang sangat rendah. Adapun variabel Kepemimpinan dan Manajemen Kebijakan Organisasi tidak memberikan dampak yang signifikan, dengan nilai F-Square sebesar 0,000.

Tabel 7. F-Sequare

Variable	Cyber Security Behaviour
Email Management	0.036
Infrastructure Security Management	0.031
Organizational Policy Management	0.000
Organizational Support & Training	0.003
Password Management	0.109
Perception Of Security	0.005

Sumber : Data Olahan Peneliti (2025)

Hasil uji Q-Square yang ditampilkan dalam Tabel 8 menunjukkan bahwa variabel Perilaku Keamanan Siber memiliki nilai Q^2 sebesar 0,690, yang mengindikasikan kemampuan prediktif model yang tinggi terhadap variabel tersebut. Artinya, 69% variasi dalam perilaku keamanan siber pegawai dapat dijelaskan oleh model, sementara sisanya sebesar 31% dipengaruhi oleh faktor-faktor di luar model. Sebaliknya, variabel lainnya seperti Manajemen Email, Manajemen Keamanan Infrastruktur, Kepemimpinan, Manajemen Kebijakan Organisasi, Dukungan dan Pelatihan Organisasi, Manajemen Kata Sandi, serta Persepsi terhadap Keamanan, seluruhnya memiliki nilai Q^2 sebesar 0,000. Hal ini menunjukkan bahwa variabel-variabel tersebut berperan sebagai prediktor dalam model, namun tidak memiliki kemampuan prediktif secara mandiri. Temuan ini menegaskan bahwa fokus utama prediksi dalam model ini terletak pada variabel Perilaku Keamanan Siber.

Tabel 8. Q-Sequare

Variable	Q Square
Cyber Security Behaviour	0.690
Email Management	0.000
Infrastructure Security Management	0.000
Leadership	0.000
Organizational Policy Management	0.000
Organizational Support & Training	0.000
Password Management	0.000
Perception Of Security	0.000

Sumber : Data Olahan Peneliti (2025)

C. Hipotesis

Hasil uji hipotesis ini menunjukkan bahwa *Infrastructure Security Management, Password Management,* dan *Email Management* memiliki pengaruh yang signifikan terhadap *Cyber Security Behaviour, sementara Leadership, Organizational Policy Management, Organizational Support & Training, dan Perception of Security* tidak berpengaruh secara signifikan. Temuan ini menegaskan bahwa pengelolaan infrastruktur keamanan yang baik, penggunaan kata sandi yang kuat, dan manajemen email yang aman merupakan faktor utama dalam membentuk perilaku keamanan siber pegawai pemerintah, sedangkan faktor lain mungkin memerlukan strategi tambahan agar lebih efektif dalam meningkatkan kesadaran dan kepatuhan terhadap keamanan siber.

Tabel 9. Hipotesis

Variabel	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (|O/STDEV|)	P values	Hasil
Infrastructure Security Management -> Cyber Security Behaviour	0.291	0.300	0.099	2.931	0.002	H1 Diterima
Organizational Policy Management -> Cyber Security Behaviour	0.044	0.024	0.281	0.156	0.427	H2 Ditolak
Organizational Support & Training -> Cyber Security Behaviour	-0.076	-0.043	0.145	0.526	0.253	H3 Ditolak
Password Management -> Cyber Security Behaviour	0.748	0.677	0.300	2.497	0.006	H4 Diterima

Email Management -> Cyber Security Behaviour	0.170	0.165	0.061	2.793	0.003	H5 Diterima
Perception Of Security -> Cyber Security Behaviour	-0.198	-0.137	0.192	1.027	0.152	H6 Ditolak
Leadership -> Cyber Security Behaviour	0.291	0.300	0.099	2.931	0.002	H7 Ditolak

Sumber : Data Olahan Peneliti (2025)

V. KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian, ditemukan bahwa dari enam variabel manajemen keamanan informasi yang diuji, hanya tiga yang memiliki pengaruh signifikan terhadap perilaku keamanan siber pegawai sektor pemerintahan, yaitu *Infrastructure Security Management*, *Password Management, dan Email Management*. Ketiga variabel ini ditunjukkan dengan nilai p-value < 0.05 dan statistik t yang tinggi, sedangkan variabel lainnya seperti *Organizational Policy Management, Organizational Support & Training, dan Perception of Security* tidak berpengaruh signifikan.

Temuan ini diperkuat oleh analisis deskriptif yang menunjukkan masih lemahnya penerapan perlindungan infrastruktur seperti firewall, anti-spyware, dan pembaruan sistem yang belum optimal. Dalam aspek manajemen kata sandi, pegawai cenderung menggunakan kata sandi yang sama dan jarang menggantinya secara berkala. Sementara itu, dari sisi pengelolaan email, masih banyak pegawai yang belum terbiasa memverifikasi pengirim, mengecek lampiran, dan menggunakan enkripsi saat mengirim data sensitif.

Untuk meningkatkan perilaku keamanan siber, organisasi pemerintah disarankan fokus pada penguatan tiga aspek utama tersebut. Langkah konkret yang dapat dilakukan antara lain penerapan firewall dan anti-spyware resmi, pembaruan sistem secara berkala, sosialisasi pembuatan kata sandi yang kuat dan unik, serta pelatihan penggunaan aplikasi pengelola kata sandi. Selain itu, penting untuk membiasakan penggunaan enkripsi dalam komunikasi email guna menjaga kerahasiaan data. Pelatihan teknis yang berkelanjutan, penyediaan panduan sederhana, dan monitoring rutin menjadi kunci untuk membentuk budaya keamanan informasi yang konsisten. Evaluasi berkala terhadap kepatuhan pegawai juga diperlukan agar kebijakan keamanan yang diterapkan dapat berjalan efektif dalam jangka panjang.

Penelitian selanjutnya disarankan untuk mengeksplorasi lebih dalam variabel yang tidak signifikan menggunakan pendekatan studi kasus atau metode kualitatif. Selain itu, perluasan objek penelitian dengan melibatkan lebih banyak instansi dari berbagai wilayah serta penggunaan pendekatan longitudinal akan memberikan pemahaman yang lebih komprehensif tentang efektivitas strategi keamanan siber di lingkungan pemerintahan Indonesia.

REFERENSI

Alghazo, S. H. A., Humaidi, N., & Noranee, S. (2023). Assessing Information Security Competencies of Firm Leaders towards Improving Procedural Information Security Countermeasure: Awareness and Cybersecurity Protective Behavior. *Information Management and Business Review*, *15*(1), 119–121.

Andriessen, J., Schaberreiter, T., & Papanikolaou, A. (2022). *Cybersecurity Awareness* (Juha Röning (ed.)). Springer.

Anto, C. A. S. (2024). *"PDN Diretas Berhari-hari, Bagaimana Nasib Data Pribadi Kita?,."* Kompas. https://www.kompas.id/baca/polhuk/2024/06/27/pdn-diretas-bagaimana-nasib-data-pribadi-kita

Azizi, A. F., Tahir, M., Iriansyah, M. D. P., Kusumawati, W., Rahayu, R., Setyaningrum, R., & Ananta, W. O. (2024). ANALISIS PENTINGNYA EDUKASI KEAMANAN SIBER BAGI PENGGUNA MAHASISWA. *Esensi Pendidikan Inspirati*, *Vol. 6 No.*

BSSN. (2023). Lanskap Keamanan Siber Indonesia. *BSSN*, *70*, 1–107.

Candiwan, C., Azmi, M., & Alamsyah, A. (2022). Analysis of Behavioral and Information Security Awareness among Users of Zoom Application in COVID-19 Era. *International Journal of Safety and Security Engineering*, *12*(2), 229–237. https://doi.org/10.18280/ijsse.120212

Ciekanowski, Z., Nowicka, J., Czternastek, M., Zurawski, S., & Mikosik, P. (2024). How Cybersecurity Shapes Effective Organizational Management. *European Research Studies Journal*, *XXVII*(Issue 2), 454–464. https://doi.org/10.35808/ersj/3411

Diskominfo Bandung. (n.d.). *Sempat Diretas, Diskominfo Kota Bandung Pastikan Website Resmi Kembali Normal*. Diskominfo Bandung. https://jabarprov.go.id/berita/sempat-diretas-diskominfo-kota-bandung-pastikan-website-resmi-kembali-normal-11442

Ernita, H., Ruldeviyani, Y., Nurul Maftuhah, D., & Mulyadi, R. (2022). Strategy to Improve Employee Security Awareness at Information Technology Directorate Bank XYZ. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *6*(4), 577–584. https://doi.org/10.29207/resti.v6i4.4170

Fadlika, R., Ruldeviyani, Y., Butarbutar, Z. T., Istiqomah, R. A., & Fariz, A. A. (2023). Employee Information Security Awareness in the Power Generation Sector of PT ABC. *International Journal of Advanced Computer Science and Applications*, *14*(4), 594–603. https://doi.org/10.14569/IJACSA.2023.0140465

Grassegger, T., & Nedbal, D. (2021). The role of employees' information security awareness on the intention to resist social engineering. *Procedia Computer Science*, *181*(2019), 59–66. https://doi.org/10.1016/j.procs.2021.01.103

Intan, R., & Yasin, M. (2024). Transformasi Pada Era Disrupsi Hingga Terjadinya Revolusi Industri 4.0. *Jurnal Ekonomi Dan Pembangunan Indonesia*, *2*(3), 21–28. https://doi.org/10.61132/jepi.v2i3.650

Laudon, Kenneth C., and J. P. L. (2016). Management Infromation Systems. In *Management Information Systems: Managing the Digital Firm* (Fourteenth).

Maheswara, A. D. (2023). *Sektor Pemerintahan Masih Rawan Serangan Siber*. Detik.Com. https://inet.detik.com/security/d-6901921/sektor-pemerintahan-masih-rawan-serangan-siber

Nurse, J. R. C. (2021). Cybersecurity Awareness. *Encyclopedia of Cryptography, Security and Privacy*, 1–4. https://doi.org/10.1007/978-3-642-27739-9_1596-1

Priyatna, S. A. (2022). BIROKRASI DAN PELAYANAN PUBLIK DALAM PERSPEKTIF HUKUM ADMINISTRASI NEGARA. *DJKN*. https://www.djkn.kemenkeu.go.id/artikel/baca/15537/BIROKRASI-DAN-PELAYANAN-PUBLIK-DALAM-PERSPEKTIF-HUKUM-ADMINISTRASI-NEGARA.html

Rocha Flores, W., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers and Security*, *59*, 26–44. https://doi.org/10.1016/j.cose.2016.01.004

Sari, P. K., Candiwan, & Trianasari, N. (2014). Information security awareness measurement with confirmatory factor analysis. ISTMET 2014 - 1st International Symposium on Technology Management and Emerging Technologies,218–223. https://doi.org/10.1109/ISTMET.2014.6936509

Saeed, S. (2023a). Digital Workplaces and Information Security Behavior of Business Employees: An Empirical Study of Saudi Arabia. *Sustainability (Switzerland)*, *15*(7). https://doi.org/10.3390/su15076019

Saeed, S. (2023b). Education, Online Presence and Cybersecurity Implications: A Study of Information Security Practices of Computing Students in Saudi Arabia. *Sustainability (Switzerland)*, *15*(12). https://doi.org/10.3390/su15129426

Sekaran, U., & Bougie, R. (2016). *Research methods for business : a skill-building approach*. 1–23.

Suryadi, S. (2019). Peranan Perkembangan Teknologi Informasi Dan Komunikasi Dalam Kegiatan Pembelajaran Dan Perkembangan Dunia Pendidikan. *Jurnal Informatika*, *3*(3), 9–19.

https://doi.org/10.36987/informatika.v3i3.219
Yassen, K. (2023). The Impact of the Information Security Policies on Organizational Performance. *International Journal of Engineering and Management Research*, *13*(5), 73–78. https://doi.org/10.31033/ijemr.13.5.12
Yel, M. B., & Nasution, M. K. M. (2022). Keamanan Informasi Data Pribadi Pada Media Sosial. *Jurnal Informatika Kaputama (JIK)*, *6*(1), 92–101. https://doi.org/10.59697/jik.v6i1.144