ANALISIS MODEL HOT-FIT TERHADAP KINERJA KEAMANAN SIBER DENGAN MEDIASI KESIAPAN KEAMANAN SIBER DI RSUD AJIBARANG

[1]Agustyarum Pradiska Budi*, [2]Sri Wulandari, [3]Galuh Nugrahaning Budi
[1,2]Politeknik Indonusa Surakarta, [3]RSUD Ajibarang
Email: [1]agustyarum@poltekindonusa.ac.id*

Submitted : 04 Januari 2025 Reviewed : 27 Januari 2025 Accepted : 17 Februari 2025

ABSTRAK

Penelitian ini bertujuan mengkaji faktor-faktor HOT-FIT yaitu Human, Organization dan Technology untuk mengukur kinerja keamanan siber yang dimediasi oleh variabel kesiapan keaman siber di RSUD Ajibarang. Hasil analisis menggunakan pendekatan Partial Least Squares-Structural Equation Modeling (PLS-SEM) menunjukkan nilai R Square untuk kesiapan keamanan siber sebesar 0,768 dan kinerja keamanan siber sebesar 0,624, mengindikasikan model memiliki kekuatan eksplanatori yang baik. Namun, nilai Q Square untuk kesiapan keamanan siber (0,512) dan kinerja keamanan siber (0,256) menunjukkan kemampuan prediktif yang bervariasi. Dari 13 hipotesis yang diuji, 4 diterima, termasuk pengaruh signifikan kebijakan dan prosedur, komitmen manajemen, serta implementasi teknologi terhadap kesiapan keamanan siber, dan pengaruh sistem dan teknologi terhadap kinerja keamanan siber. Penelitian ini menyimpulkan bahwa pentingnya aspek kebijakan, komitmen manajemen, implementasi teknologi, dan sistem keamanan dalam meningkatkan kesiapan dan kinerja keamanan siber untuk peningkatan keamanan siber pada RSUD Ajibarang. Oleh karena itu rekomendasi yang diberikan untuk kesiapan keamanan siber sebagai upaya prioritas melalui dukungan manajemen terhadap kebijakan, investasi teknologi dan investasi divisi IT. Sedangkan untuk kinerja kemanan siber hanya dapat diukur melalui invetasi pemutakhiran sistem dan teknologi. Untuk itu, RSUD Ajibarang perlu melakukan penelitian lanjutan terkait evaluasi ROI (Return on Investment) dalam system dan teknologi.

Kata Kunci : kinerja keamanan siber, kesiapan keamanan siber, PLS-SEM, rekam medis elektronik

ABSTRACT

This research aims to examine the HOT-FIT factors, namely Human, Organization and Technology to measure cyber security performance which is mediated by the cyber security readiness variable at Ajibarang Regional Hospital. The results of the analysis using the Partial Least Squares-Structural Equation Modeling (PLS-SEM) approach show an R Square value for cyber security readiness of 0.768 and cyber security performance of 0.624, indicating the model has good explanatory power. However, the Q Square values for cybersecurity readiness (0.512) and cybersecurity performance (0.256) show varying predictive abilities. Of the 13 hypotheses tested, 4 were accepted, including the significant influence of policies and procedures, management commitment, and technology implementation on cybersecurity readiness, and the influence of systems and technology on cybersecurity performance. This research concludes that the importance of policy aspects, management commitment, technology implementation, and security systems in increasing cyber security readiness and performance for improving cyber security at Ajibarang Regional Hospital. Therefore, recommendations are given for cyber security readiness as a priority effort through management support for policy, technology investment and IT division investment. Meanwhile, cyber security performance can only be measured through investment in system and technology updates. For this reason, Ajibarang Regional Hospital needs to carry out further research related to evaluating ROI (Return on Investment) in systems and technology.

Keywords: *cybersecurity performance, cybersecurity readiness, PLS-SEM, electronic medical records*

PENDAHULUAN

Kebutuhan layanan kesehatan dalam penyelenggaraan rekam medis secara elektronik atau RME didukung dengan adanya Permenkes No. 24 Tahun 2022 pada pasal 45 mewajibkan “Seluruh Fasilitas Pelayanan Kesehatan (Fasyankes) harus menyelenggarakan Rekam Medis Elektronik sesuai dengan ketentuan dalam Peraturan Menteri ini paling lambat pada tanggal 31 Desember 2023” (Sadikin, 2022). Oleh karena itu seluruh Fasyankes di Indonesia saat ini sedang berinvestasi untuk kebutuhan transformasi digital pada RME.

Informasi yang dikandung dalam RME merupakan informasi yang sangat sensitif meliputi data terkait pemeriksaan pasien, diagnosa, pengobatan serta informasi riwayat kesehatan pasien (Ikawati, Fita; Ansyori, 2023). Implementasi RME di fasyankes saat ini berada pada tahap pengembangan RME secara parsial. RME memiliki prinsip keamanan dan kerahasiaan data dan informasi. Keamanan Sistem Informasi adalah informasi merupakan salah satu aset yang penting untuk dilindungi keamanannya. Perusahaan perlu memperhatikan keamanan aset informasinya, kebocoran informasi dan kegagalan pada sistem dapat mengakibatkan kerugian baik pada sisi finansial maupun produktifitas perusahaan (Nurul, Anggrainy and Aprelyani, 2022).

Analisis kesiapan keamanan siber menggunakan metode HOTFIT melibatkan penilaian kesiapan organisasi dalam mengelola keamanan informasi (Sulistyowati, Handayani and Suryanto, 2020). Metode ini berfokus pada peningkatan pembelajaran organisasi, proses, peran, komunikasi, dan kemampuan latihan untuk meningkatkan kematangan keamanan siber (Karjalainen *et al.*, 2023). Penelitian dari (Juliantari *et al.*, 2023) menjelaskan unsur *Organization* adalah unsur yang paling tinggi kategori baik dan unsur *Technology* adalah unsur yang paling rendah. Implementasi RME tetap sangat membutuhkan persiapan, dukungan, dan keberlanjutan yang dipengaruhi faktor-faktor yang berkontribusi dalam keberhasilan implementasi RME seperti dukungan SDM, *hardware*, keuangan, pimpinan, pelatihan dan dukungan teknis.

Dalam beberapa tahun terakhir, implementasi Rekam Medis Elektronik (RME) di fasilitas pelayanan kesehatan (Fasyankes) semakin menjadi perhatian utama, terutama setelah diberlakukannya Permenkes No. 24 Tahun 2022 yang mewajibkan seluruh Fasyankes untuk menyelenggarakan RME sebelum 31 Desember 2023. Penelitian-penelitian terdahulu telah banyak berfokus pada kesiapan implementasi RME, termasuk faktor-faktor yang mempengaruhi adopsi sistem ini seperti persepsi kemudahan dan manfaat penggunaannya (Laila *et al.*, 2024). Namun, penelitian yang secara spesifik mengukur kesiapan dan kinerja keamanan siber dalam sistem RME masih sangat terbatas.

Metode HOT-FIT (Human, Organization, and Technology – Fit) telah digunakan dalam beberapa penelitian untuk menganalisis kesiapan dan efektivitas sistem informasi kesehatan. Namun, penelitian-penelitian tersebut masih belum mengkaji secara khusus keamanan siber pada RME, terbatas pada kesiapan implementasi RME di RS. Artinya, RS selama ini lebih berfokus pada kesiapan implementasi RME, seperti aspek adopsi sistem, kemudahan penggunaan, manfaat yang dirasakan, serta faktor-faktor yang mendukung keberhasilan penerapan RME. Namun, aspek keamanan siber dalam RME belum menjadi perhatian utama, sehingga evaluasi terkait kinerja keamanan siber dalam sistem RME masih terbatas.

RSUD Ajibarang saat ini telah menerapkan Sistem Informasi Manajemen Rumah Sakit (SIMRS) dan sedang dalam tahap penerapan Tanda Tangan Elektronik (TTE) untuk layanan rawat jalan dan rawat inap sejak Januari 2023. Namun, belum ada kajian komprehensif yang mengevaluasi kesiapan dan kinerja keamanan siber dalam implementasi RME di rumah sakit ini.

Penelitian ini memiliki kebaruan dengan mengintegrasikan faktor-faktor HOT-FIT dalam mengukur kinerja keamanan siber dengan mempertimbangkan kesiapan keamanan siber sebagai variabel mediasi. Pendekatan ini belum banyak ditemukan dalam penelitian sebelumnya, sehingga dapat memberikan kontribusi akademik dan praktis dalam meningkatkan keamanan informasi dalam sistem RME di Indonesia.

METODE

Desain penelitian di RSUD Ajibarang ini berupaya mengkaji secara kritis variabel infrastruktur IT, keterampilan pegawai, dukungan pimpinan, dan budaya kerja terhadap kolaborasi dan peran mediasi variabel kesiapan *cyber security* dalam hubungannya dengan variabel kinerja *cyber security* di RSUD Ajibarang. Penelitian ini termasuk dalam jenis penelitian kuantitatif dengan pendekatan deskriptif.

Populasi dalam penelitian ini terbagi menjadi beberapa unit kerja terkait dalam keamanan siber. Populasi penelitian berdasarkan pembagian unit kerja (tenaga medis sejumlah 500, rekam medis sejumlah 34, dan tim IT sejumlah 12). Total populasi sebesar 546 orang. Pengambilan sampel menggunakan teknik sampel **slovin** dan memetakan kesiapan dari lapisan atau kategori tenaga medis dan non medis. Jumlah sampel yang dihitung menggunakan perhitungan slovin sebagai berikut:

$$n = \frac{\mathrm{N}}{1 + N.e^2}$$

$$n = \frac{546}{1 + 546\ .0{,}10^2}$$

$$n = \frac{546}{1 + 546.0{,}01}$$

$$n = \frac{546}{1 + 5{,}46}$$

$$n = \frac{546}{6{,}46}$$

= 84,5

= 85 (pembulatan)

Pengukuran kinerja *cyber security* menggunakan 1 variabel mediasi dan 6 variabel bebas. Kinerja *cyber security* sebagai variabel terikat diukur melalui mediasi oleh variabel kesiapan *cyber security* dan 6 variabel bebas. Perolehan variabel bebas menggunakan metode HOT-FIT. Faktor *Human* diwakili oleh variabel Keterampilan Karyawan, dan Kesadaran *Cyber Security.* Faktor *Organization* terdapat Variabel Kebijakan dan Prosedur Keamanan, dan Komitmen Manajemen dan Kepemimpinan. Faktor *Technology* diukur menggunakan Variabel Sistem dan Teknologi Keamanan, dan Implementasi dan Pemeliharaan Teknologi.

Berdasarkan dari kerangka HOT-FIT, variabel-variabel yang telah dijelaskan menghasilkan 13 hipotesis terbagi menjadi pengujian 6 variabel bebas terhadap kesiapan *cyber security*, 6 variabel bebas terhadap kinerja *cyber security* dan 1 menguji hubungan positif antara kesiapan *cyber security* dan kinerja *cyber security*. Jenis data yang akan diperoleh merupakan data primer dengan teknik pengumpulan data menggunakan kuesioner. Kuesioner disusun mengadopsi skala likert dengan 7 skala respon.

Analisis data menggunakan Analisis *Partial Least Square* (PLS) Penelitian ini menggunakan model persamaan *Partial Least Square Structural Equation Model* (PLS-SEM) dan khususnya pemodelan persamaan struktural berbasis varians. PLS-SEM merupakan metode yang tepat karena tidak didasarkan banyak asumsi. Teknik analisis data menggunakan perangkat lunak Smart PLS (Pejić Bach *et al.*, 2023).

HASIL DAN PEMBAHASAN

Pengukuran kinerja keamanan siber pada RME di RSUD Ajibarang menggunakan metode HOT-FIT terdiri dari variabel keterampilan karyawan, kesadaran, kebijakan dan prosedur keamanan, komitmen manajemen dan kepemimpinan, sistem dan teknologi keamanan, implementasi dan pemeliharaan teknologi yang dimediasi oleh kesiapan *cyber security*. Sejumlah 85 responden yang terdiri dari tenaga medis, petugas rekam medis, tim IT, kepala instalasi rekam medis dan kepala instalasi tim IT telah mengisi kuesioner berkaitan dengan persepsi pengguna terhadap kinerja *cyber security* di RSUD Ajibarang khususnya pada Rekam Medis Elektronik.

Analisis model HOT-FIT menggunakan metode PLS-SEM dengan dua tahapan yaitu outer model (model pengukuran) dan Inner model (Model Struktural). Outer model (model pengukuran) digunakan untuk menguji validitas dan reliabilitas. Sedangkan Inner model adalah langkah kedua yang merupakan pengukuran struktural model. Model pengukuran menggambarkan bagaimana konstruk dinilai menggunakan indikator. Validitas dan reliabilitas Indikator yang digunakan dalam analisis multivariat harus dikonfirmasi oleh peneliti agar dapat meningkatkan akurasi pengukuran.

1. Analisis Model Pengukuran *(Outer Loading)*

Jika nilai dari outer loading lebih besar dari (0.5) maka suatu indikator adalah valid. Hasil validitas konvergen menunjukkan bahwasanya nilai dari outer loading dari masing-masing indikator lebih besar dari 0.5 semua indikator adalah valid (Nasution and Chairunnisa, 2023). Pengukuran validitas selain dari nilai loading factor, juga dapat dilihat dari nilai *Average Variance Extracted* (AVE). Validitas diskriminan ditunjukkan dengan menguji apakah nilai AVE lebih dari 0,5.

Tabel 1. Hasil Convergent Validity

Variabel	Indikator	Loading Factor	AVE
Keterampilan Karyawan	KK1	0,840	0,699
	KK2	0,747	
	KK3	0,923	
	KK4	0,865	
	KK5	0,833	
	KK6	0,798	
Kesadaran Cyber Security	KS1	0,792	0,612
	KS2	0,798	
	KS3	0,807	

Variabel	Indikator	Loading Factor	AVE
	KS4	0,780	
	KS5	0,809	
	KS7	0,803	
	KS8	0,677	
Kebijakan dan Prosedur	KP1	0,832	0,662
	KP2	0,841	
	KP3	0,724	
	KP4	0,817	
	KP5	0,847	
	KP6	0,812	
Komitmen Manajemen dan Kepemimpinan	KMP1	0,833	0,676
	KMP2	0,893	
	KMP3	0,793	
	KMP4	0,797	
	KMP5	0,823	
	KMP6	0,788	
Sistem dan Teknologi Keamanan	STK1	0,559	0,556
	STK2	0,751	
	STK3	0,759	
	STK4	0,847	
	STK5	0,877	
	STK6	0,629	
Implementasi dan Pemeliharaan Teknologi	IMP1	0,865	0,773
	IMP2	0,863	
	IMP3	0,910	
Kesiapan Cyber Security	KES1	0,858	0,692
	KES2	0,880	
	KES3	0,808	
	KES4	0,767	
	KES5	0,844	
	KES6	0,829	
Kinerja Cyber Security	KIN1	0,652	0,501
	KIN2	0,710	
	KIN3	0,680	
	KIN4	0,763	
	KIN5	0,730	

Sumber: Data Primer yang diolah menggunakan SmartPLS3.0

Hasil validitas konvergen pada tabel 1 merupakan hasil setelah melakukan 2 eliminasi indikator yang tidak memenuhi syarat yaitu indikator 6 dari Kesadaran *Cyber Security* (KS6) dan indikator 6 dari Kinerja *Cyber Security.* Tabel 1 dipastikan seluruh item Valid karena tidak ada indikator dengan nilai loading factor di bawah 0,5 (keseluruhan loading factor > 0,5). Table 1 menunjukkan bahwa keseluruhan nilai AVE > 0,50, sehingga persyaratan uji validitas dinyatakan memenuhi.

Selanjutnya uji reliabilitas variable diukur dengan dua aspek yaitu cronbach's alpha dan composite reliability. Nilai cronbach's alpha > 0,6 dan nilai composite reliability > 0,7 agar variabel dapat dikatakan reliabel. Berikut tabel hasil pengukuran reliability:

Tabel 2. Hasil Reliability

Variabel	Cronbach Alpha	Composite Reliability
Implementasi dan Pemeliharaan	0,853	0,911
Kebijakan dan Prosedur	0,897	0,921
Kesadaran CS	0,894	0,917
Kesiapan CS	0,910	0,931
Keterampilan Karyawan	0,913	0,933
Kinerja CS	0,751	0,834
Komitmen Manajaemen	0,904	0,926
Sistem dan Teknologi	0,833	0,880

Sumber: Data Primer yang diolah menggunakan SmartPLS3.0

Output reliability melalui Cronbach alpha pada tabel 2 memiliki nilai di atas 0,6 dan nilai composite reliability di atas 0,7. Artinya seluruh variabel telah memenuhi syarat uji reliability. Peneliti dapat melanjutkan ke tahap selanjutnya yaitu dilakukan uji validitas diskriminan *(discriminant validity)* yang dinilai berdasarkan Fornell-Larcker Criterion dengan membandingkan akar kuadrat dari AVE untuk setiap konstruk dengan nilai korelasi antar konstruk dalam model. Hasil Fornell-Larcker Criterion dapat disimpulkan bahwa nilai akar AVE untuk setiap konstruknya lebih tinggi dari pada korelasi setiap konstruk dengan konstruk lainnya. Seperti pada konstruk Implementasi dan Pemeliharaan memiliki nilai akar AVE sebesar 0,879 yakni lebih besar daripada korelasi dengan konstruk lainnya (0,701; 0,705; 0,753; 0,739; 0,625; 0,699; 0,693).

2. Analisis Struktural Model *(Inner Model)*

Inner model digunakan untuk menguji model structural sebanyak 86 responden yang dinilai berdasarkan nilai R^2 pada variabel endogen (variabel dependen). Hasil R^2 sebagai berikut:

Tabel 3. Hasil R-Square (R^2)

	R Square
Kesiapan CS	0,768
Kinerja CS	0,624

Sumber: Data Primer yang diolah menggunakan SmartPLS3.0

Nilai R-Square sebesar 0,768 menunjukkan bahwa 76,8% variasi kesiapan *cyber security* dapat dijelaskan oleh variabel-variabel independen yang digunakan dalam model penelitian. Ini menunjukkan bahwa model memiliki kemampuan prediktif yang sangat baik dalam menjelaskan kesiapan *cyber security*. Sisanya, sebesar 23,2%, dipengaruhi oleh faktor-faktor lain yang tidak dimasukkan dalam model.

Nilai R-Square ini mengindikasikan bahwa RME di RSUD Ajibarang telah mempertimbangkan sebagian besar faktor penting yang memengaruhi kesiapan mereka terhadap ancaman keamanan siber. Hal ini sejalan dengan penelitian terdahulu seperti yang dilakukan oleh (Sheik Ahmed and Isak Abdirahman, 2024), bahwa pelatihan reguler dan program pendidikan meningkatkan keamanan siber dengan mengajarkan kompetensi teknis terkini kepada tenaga kerja organisasi.

Nilai R-Square sebesar 0,624 menunjukkan bahwa 62,4% variasi kinerja cyber security dapat dijelaskan oleh variabel-variabel independen dalam model. Meskipun lebih rendah dibandingkan kesiapan, nilai ini masih menunjukkan hubungan yang cukup kuat antara variabel prediktor dan kinerja keamanan siber. Nilai ini mencerminkan bahwa kinerja *cyber security* dipengaruhi oleh faktor-faktor internal dan eksternal, namun tidak semuanya terukur dalam model penelitian.

Tahapan *inner model* yang kedua yaitu menghitung Q^2 dimana berguna untuk mengukur seberapa baik path model dapat memprediksi nilai-nilai data aslinya. Berikut tabel 5 merupakan hasil perhitungan Q^2 dalam penelitian ini:

Tabel 4. Hasil Perhitungan Q-Square (Q^2)

	Q^2 (=1-SSE/SSO)
Kesiapan CS	0,512
Kinerja CS	0,256

Sumber: Data Primer yang diolah menggunakan SmartPLS3.0

Berdasarkan tabel 5 di atas nilai variabel mediasi (Z) sebesar 0,512 > 0 dan variabel Y sebesar 0,256 > 0. Hal tersebut menunjukkan bahwa variabel bebas telah sesuai sebagai variabel penjelas yang mampu memprediksi variabel Y. Nilai Q-Square pada Kesiapan *Cyber Security* sebesar 0,512, variabel kesiapan cyber security memiliki kekuatan prediktif yang moderat hingga kuat. Artinya, variabel bebas cukup mampu menjelaskan kesiapan *cyber security* dalam konteks ini. Nilai Q-Square Kinerja *Cyber Security* sebesar 0,256 bahwa 25,6% variansi kinerja cyber security dapat dijelaskan oleh variabel bebas dan variabel mediasi. Nilai 0,256, model memiliki kekuatan prediktif yang lemah hingga moderat untuk menjelaskan kinerja *cyber security*.

Setelah melihat nilai Q2 selanjutnya melakukan uji hipotesis dengan *path coefficients*. Pengujian hipotesis dapat dilihat dari besarnya nilai t-statistik. Nilai t-statistik diatas 1,96 untuk pengujian hipotesis pada alpha 5% dinyatakan hipotesis diterima.

Tabel 5. Output Uji Hipotesis (*Direct Relationship*)

Hi	Paths	OS	T	P-Values	Ket
H1	Keterampilan -> Kesiapan CS	0,103	0,565	**0,572**	Ditolak
H2	Kesadaran -> Kesiapan CS	-0,167	0,920	**0,358**	Ditolak
H3	Kebijakan dan Prosedur -> Kesiapan CS	0,228	1,977	**0,049**	Diterima

Hi	Paths	OS	T	P-Values	Ket
H4	Komitmen -> Kesiapan CS	0,471	3,624	**0,000**	Diterima
H5	Sistem dan Teknologi -> Kesiapan CS	0,117	1,052	**0,293**	Ditolak
H6	Implementasi dan Pemeliharaan -> Kesiapan CS	0,224	2,090	**0,037**	Diterima
H7	Keterampilan Karyawan -> Kinerja CS	-0,114	0,581	**0,562**	Ditolak
H8	Kesadaran CS -> Kinerja CS	-0,007	0,032	**0,974**	Ditolak
H9	Kebijakan dan Prosedur -> Kinerja CS	0,135	0,754	**0,451**	Ditolak
H10	Komitmen Manajemen -> Kinerja CS	0,139	0,634	**0,526**	Ditolak
H11	Sistem dan Teknologi -> Kinerja CS	0,355	2,588	**0,010**	Diterima
H12	Implementasi dan Pemeliharaan -> Kinerja CS	0,017	0,108	**0,914**	Ditolak
H13	Kesiapan CS -> Kinerja CS	0,345	1,676	**0,094**	Ditolak

Sumber: Data Primer yang diolah menggunakan SmartPLS3.0

Hasil temuan pada perhitungan PLS-SEM bahwa berdasarkan 13 hipotesis yang diusulkan, terdapat 4 variabel yang diterima dan 9 variabel ditolak. Nilai yang digunakan untuk menguji hipotesis diantaranya koefisien jalur, nilai t, dan nilai p pada tingkat signifikansi 0,05. Hipotesis yang diterima yaitu H3, H4, H6 dan H11. Hipotesis 3, 4 dan 6 menguji secara langsung antara variabel bebas dengan variabel mediasi. Hipotesis 3 menunjukkan hubungan langsung antara kebijakan dan prosedur dengan kesiapan *cyber security* diterima. Kebijakan dan prosedur keamanan yang baik memiliki kontribusi signifikan (0,049) dan positif dalam meningkatkan kesiapan *cyber security*. Hal ini menunjukkan bahwa organisasi yang memiliki regulasi internal, SOP, dan panduan keamanan yang jelas lebih mampu membangun kesiapan dalam menghadapi ancaman siber. (Departemen Penelitian dan Pengaturan Perbankan Otoritas Jasa Keuangan, 2021)

Ditemukan terdapat hubungan langsung yang signifikan (0,000) dan positif antara komitmen manajemen dengan kesiapan *cyber security* diterima (Hipotesis 4). Selain dukungan kebijakan yang baik, temuan ini menunjukkan bahwa kesiapan *cyber security* sangat bergantung pada dukungan aktif dari manajemen puncak. Komitmen manajemen yang tinggi, seperti alokasi sumber daya, pelatihan, dan pengawasan, berpengaruh signifikan terhadap kesiapan organisasi dalam menghadapi ancaman siber.

Implementasi dan pemeliharaan teknologi dengan kesiapan cyber security memiliki hubungan langsung yang signifikan (0,037) dan positif, sehingga hipotesis 6 diterima. Variabel ini mengukur kesiapan implementasi sistem yang dapat dikembangkan sesuai kebutuhan dengan biaya yang efektif dan sesuai dengan standar keamanan. RSUD Ajibarang memiliki persepsi bahwa implementasi dan pemeliharaan teknologi harus disesuaikan dengan kebutuhan organisasi memiliki hubungan dengan kesiapan *cyber security*. Implementasi teknologi yang relevan dan pemeliharaan yang berkelanjutan memainkan peran penting dalam kesiapan menghadapi ancaman siber. Sistem keamanan yang tidak hanya diterapkan tetapi juga diperbarui secara rutin memberikan kontribusi besar dalam memastikan kesiapan organisasi. (Hoshmand, Ratnawati and Korespondensi, 2023)

Pengujian secara langsung pada variabel bebas dan variabel terikat (kinerja *cyber security*) terdapat 1 hipotesis yang diterima yaitu hipotesis 11. Hubungan langsung yang siginifikan (0,010) dan positif pada sistem dan teknologi keamanan dengan kinerja cyber security di RSUD Ajibarang. Sistem dan teknologi yang canggih, seperti firewall, enkripsi, atau sistem deteksi intrusi, secara langsung meningkatkan kinerja keamanan siber organisasi. Hal ini menunjukkan bahwa investasi dalam infrastruktur teknologi memberikan dampak nyata terhadap kemampuan organisasi untuk melindungi aset digitalnya. Menurut National Institute of Standards and Technology (NIST), melalui proses peningkatan berkelanjutan dengan memasukkan teknologi maju dan praktik keamanan siber, organisasi secara aktif beradaptasi terhadap perubahan lanskap ancaman dan teknologi. (Pratomo *et al.*, 2018)

KESIMPULAN

Berdasarkan hasil dan pembahasan, variabel kesiapan cyber security menunjukkan bahwa 76,8% variabilitas kesiapan keamanan siber dapat dijelaskan oleh variabel independen dalam model dan model memiliki kemampuan prediktif yang baik untuk variabel kesiapan keamanan siber. Sedangkan kinerja cyber security menunjukkan bahwa 62,4% variabilitas kinerja keamanan siber dapat dijelaskan oleh variabel dalam model, namun memiliki kemampuan prediktif yang sedang untuk variabel kinerja keamanan siber.

Dari 13 hipotesis yang diuji, hanya 4 yang diterima (signifikan), sementara 9 lainnya ditolak. Hal ini menunjukkan bahwa tidak semua variabel independen memiliki pengaruh signifikan terhadap variabel dependen dalam model ini. Pada bab hasil dan pembahasan telah dibahas satu per satu hasil dari keempat hipotesis yang diterima. Oleh karena itu, penulis menarik kesimpulan temuan ini menegaskan pentingnya aspek kebijakan, komitmen manajemen, implementasi teknologi, dan sistem keamanan dalam meningkatkan kesiapan dan kinerja keamanan siber organisasi untuk peningkatan keamanan siber pada RSUD Ajibarang.

Saran yang diberikan diantaranya RSUD Ajibarang perlu melakukan evaluasi dan pembaruan berkala terhadap kebijakan dan prosedur untuk memastikan relevansinya dengan ancaman terkini dan memprioritaskan sosialisasi agar seluruh karyawan memahami peran mereka dalam kesiapan *cyber security*. Hal ini juga sekaligus menunjukkan adanya komitmen dari manajemen melalui kebijakan strategis, investasi teknologi, dan komunikasi yang mendorong budaya keamanan di seluruh RSUD Ajibarang.

Variabel implementasi dan pemeliharaan membutuhkan penguatan divisi IT yang bertugas melakukan audit teknologi secara berkala untuk memastikan bahwa sistem tetap optimal dan tangguh terhadap ancaman baru. Kinerja *cyber security* dalam penelitian ini kurang bisa diukur melalui variabel bebas dan variabel mediasi, hanya 1 variabel bebas yang memiliki hubungan yaitu sistem dan teknologi. Hal ini menunjukkan kinerja baik dan buruknya *cyber security* hanya dapat diukur melalui invetasi pemutakhiran sistem dan teknologi. Untuk itu, RSUD Ajibarang perlu melakukan penelitian lanjutan terkait evaluasi ROI (Return on Investment) untuk memastikan bahwa investasi teknologi memberikan manfaat nyata terhadap kinerja keamanan.

UCAPAN TERIMA KASIH

Penulis mengucapkan rasa syukur dan terima kasih yang sebesar-besarnya kepada semua pihak yang telah berkontribusi dalam mendukung pelaksanaan penelitian ini, yang berjudul "Faktor-Faktor yang Mempengaruhi Kinerja Cyber Security dalam RME yang Dimediasi oleh Kesiapan Cyber Security". Secara khusus, penulis menyampaikan penghargaan dan terima kasih kepada Politeknik Indonusa Surakarta yang telah memberikan dukungan finansial melalui pendanaan penelitian ini. Selain itu juga kepada RSUD Ajibarang yang telah memberikan kesempatan dan fasilitas untuk melaksanakan penelitian. Kerjasama yang baik dari pihak manajemen rumah sakit, serta bantuan dari staf dan tenaga medis, sangat membantu penulis dalam pengumpulan data dan pelaksanaan penelitian di lapangan.

DAFTAR PUSTAKA

Departemen Penelitian dan Pengaturan Perbankan Otoritas Jasa Keuangan (2021) ‘Manajemen Risiko Keamanan Siber Bank Umum Departemen’, p. 75.

Hoshmand, M.O., Ratnawati, S. and Korespondensi, E.P. (2023) ‘Analisis Keamanan Infrastruktur Teknologi Informasi dalam Menghadapi Ancaman Cybersecurity’, *Jurnal Sains dan Teknologi*, 5(2), pp. 679–686. Available at: https://doi.org/10.55338/saintek.v5i2.2347.

Ikawati, Fita; Ansyori, A. (2023) ‘TANTANGAN REKAM MEDIS ELEKTRONIK DALAM PERLINDUNGAN DATA PRIBADI CHALLENGES OF ELECTRONIC MEDICAL RECORDS IN’, *Prosiding Seminar Nasional Rekam Medis & Manajemen Informasi Kesehatan*, pp. 10–18.

Juliantari, N.K. *et al.* (2023) ‘Gambaran Proses Implementasi Rekam Medis Elektronik Di Unit Rawat Jalan Dengan Metode Hot-Fit Di Rumah Sakit Umum Ari Canti’, *The Journal of Management Information and Health Technology*, 1(1), pp. 29–34. Available at: https://www.ejournal.politeknikkesehatankartinibali.ac.id/index.php/maintekkes/article/view/12.

Karjalainen, M. *et al.* (2023) ‘Learn to Train Like You Fight’, *International Journal of Adult Education and Technology*, 14(1). Available at: https://doi.org/10.4018/ijaet.322085.

Laila, M.I.K. *et al.* (2024) ‘Faktor Penghambat Pelaksanaan Rekam Medis Elektronik Di Rumah Sakit: Narrative Review’, *... Informasi Kesehatan ...*, pp. 65–71. Available at: https://doi.org/10.33560/jmiki.v12i1.645.

Nasution, S.W. and Chairunnisa, C. (2023) ‘Hospital Management Information System Implementation Assessment Using HOT-FIT Model in Langsa General Hospital Aceh, Indonesia’, *Majalah Kedokteran Bandung*, 55(1), pp. 13–20. Available at: https://doi.org/10.15395/mkb.v55n1.280.

Nurul, S., Anggrainy, S. and Aprelyani, S. (2022) ‘Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi : Keamanan Informasi , Teknologi Informasi Dan Network (Literature Review Sim)’, *Jurnal Ekonomi Manajemen Sistem Informasi (Jemsi)*, Vol. 3(No. 5), pp. 564–573.

Pejić Bach, M. *et al.* (2023) ‘Supply Chain Management Maturity and Business Performance: The Balanced Scorecard Perspective’, *Applied Sciences (Switzerland)*, 13(4), pp. 1–24. Available at: https://doi.org/10.3390/app13042065.

Pratomo, B.A. *et al.* (2018) ‘Kerangka Kerja untuk Meningkatkan Keamanan Siber Infrastruktur Kritis’, *National Institute of Standards and Technology*, 1.1(April), pp. 1–51.

Sadikin, B. (Menteri K.R.I. (2022) ‘Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022’, *Menteri Kesehatan Republik Indonesia*. Jakarta: Menteri Kesehatan Republik Indonesia, pp. 1–12.

Sheik Ahmed, S.A.A. and Isak Abdirahman, M.A. (2024) ‘Factors Affect Cyber Security Readiness and Performance of SMEs: A Case Study of Mogadishu, Somalia’, *International Journal of Innovative Science and Research Technology (IJISRT)*, 9(7), pp. 1059–1069. Available at:

https://doi.org/10.38124/ijisrt/ijisrt24jul264.

Sulistyowati, D., Handayani, F. and Suryanto, Y. (2020) 'Comparative analysis and design of cybersecurity maturity assessment methodology using nist csf, cobit, iso/iec 27002 and pci dss', *International Journal on Informatics Visualization*, 4(4). Available at: https://doi.org/10.30630/joiv.4.4.482.