Department of Digital Business
Journal of Artificial Intelligence and Digital Business (RIGGS)
Homepage: https://journal.ilmudata.co.id/index.php/RIGGS
Vol. 5 No. 2 (2026) pp: 26166-26175
P-ISSN: 2963-9298, e-ISSN: 2963-914X

Pengaruh Budaya Keamanan Siber terhadap Kinerja Karyawan dalam Sistem Transportasi Publik Digital: Studi Kasus Suroboyo Bus

Agoes Hadi Poernomo
Universitas Islam Majapahit
ahp@unim.ac.id

Abstract

The digital transformation of public transport services requires organizations not only to develop technology but also to build a strong cybersecurity culture. This article analyzes the impact of cybersecurity culture on employee performance with digital literacy as a moderating variable using Suroboyo Bus as a case study. Data were collected via a quantitative survey of 124 respondents, selected through simple random sampling from 180 active employees involved in digital operations. Cybersecurity culture was measured across four dimensions: security awareness, policy compliance, security behavior, and management support and training. Analysis was conducted using Moderated Regression Analysis (MRA). The results indicate that security awareness (X1), cybersecurity behavior (X3), and management support and security training (X4) have a positive and significant impact on performance. Conversely, security policy compliance (X2) did not have a significant effect, as compliance was largely administrative in nature and had not yet been internalized as a work behavior. Moderation testing revealed that digital literacy (M) strengthens the impact of security awareness (X1) on performance but does not moderate the relationship between cybersecurity behavior (X3) and performance. The novelty of this study lies in the integration of cybersecurity culture and digital literacy within the context of digital public transport in Indonesia a topic rarely examined empirically. These findings offer practical contributions for public sector management in designing behavior-based cybersecurity policies and enhancing employee digital literacy to support operational performance.

Keywords: Cybersecurity Culture, Digital Literacy, Employee Performance, Digital Public Transport, Suroboyo Bus.

1. Introduction

Transformasi digital telah menjadi fenomena yang tidak dapat dihindari dalam berbagai sektor organisasi, termasuk transportasi publik. Pemanfaatan teknologi seperti sistem tiket elektronik, Internet of Things (IoT), perangkat mobile untuk operasional, dan manajemen data pelanggan menjadi bagian dari layanan modern yang dihadapi organisasi transportasi publik. Dalam konteks Indonesia, organisasi seperti Suroboyo Bus yang mengimplementasikan sistem digital dalam operasionalnya menghadapi tantangan tidak hanya soal teknis tetapi juga soal sumber daya manusia (SDM) dan bagaimana budaya organisasi mendukung keamanan siber dan kinerja karyawan.

Budaya keamanan siber (*cybersecurity culture*) menjadi aspek penting karena semakin besar ketergantungan organisasi terhadap sistem digital dan data. Budaya keamanan siber mencakup kesadaran, sikap, nilai, perilaku, dan dukungan organisasi untuk menjaga keamanan informasi serta sistem operasional dari ancaman siber. Jika budaya ini lemah, maka risiko insiden seperti kebocoran data, gangguan sistem, atau layanan digital yang tidak andal bisa meningkat yang pada gilirannya bisa berdampak pada kinerja karyawan dan kualitas layanan publik.

Penelitian terdahulu menunjukkan bahwa kesadaran keamanan, kepatuhan terhadap kebijakan, perilaku keamanan, dan dukungan manajemen & pelatihan adalah dimensi penting dari budaya keamanan siber. Misalnya, dalam konteks maritim, sebuah studi menemukan bahwa literasi digital signifikan meningkatkan kesadaran keamanan siber tetapi tidak langsung meningkatkan *resilience cyber* tanpa dukungan sistem dan teknologi yang memadai [1]. Sementara itu, literatur mengenai *digital literacy* di Indonesia menunjukkan bahwa tingkat literasi digital pekerja publik masih variatif, dan itu juga berkaitan dengan efektivitas pengimplementasian teknologi dan layanan digital [2].

Kinerja karyawan adalah variabel kritikal dalam layanan publik digital, karena karyawan yang memiliki kinerja baik akan memberikan layanan yang cepat, akurat, dan andal kepada pengguna. Dalam konteks organisasi transportasi publik digital, kinerja karyawan tidak hanya diukur dari segi operasional (misalnya tepat waktu, jumlah penumpang, efisiensi) tetapi juga dari segi digital (misalnya penggunaan aplikasi, pengelolaan data, keamanan transaksi). Beberapa penelitian di Indonesia menunjukkan bahwa digital literacy dan kompetensi digital karyawan dapat mendukung kinerja mereka dalam lingkungan yang semakin digital.

Lebih lanjut, literasi digital (*digital literacy*) sebagai kapabilitas individu dalam memahami, mengevaluasi, dan menggunakan teknologi digital dengan aman dan efektif telah diidentifikasi sebagai faktor yang dapat memperkuat hubungan antara budaya keamanan siber dan kinerja karyawan. Dalam survei nasional Indonesia, indeks literasi digital meningkat (misalnya skor 3,49 ke 3,54 pada tahun 2022) meski masih terdapat tantangan besar dalam aspek keamanan digital. Namun, sedikit sekali penelitian yang secara empiris menguji bagaimana budaya keamanan siber, literasi digital, dan kinerja karyawan saling berinteraksi dalam setting organisasi transportasi publik di Indonesia.

Penelitian ini mengangkat studi kasus Suroboyo Bus, dengan tujuan menganalisis pengaruh budaya keamanan siber terhadap kinerja karyawan, serta melihat bagaimana literasi digital memoderasi pengaruh tersebut. Penelitian ini diharapkan menawarkan kontribusi baik dari ranah akademik maupun praktis pengelolaan organisasi transportasi publik digital, khususnya di Indonesia. Penelitian ini menawarkan beberapa kontribusi: (1) mengisi gap penelitian dalam domain budaya keamanan siber dan digital literacy di sektor transportasi publik, (2) menyediakan model konseptual yang menggabungkan empat dimensi budaya keamanan siber dengan literasi digital sebagai moderator terhadap kinerja karyawan, dan (3) memberikan implikasi bagi manajemen transportasi publik dalam merancang pelatihan, kebijakan, dan struktur dukungan organisasi untuk meningkatkan kinerja melalui penguatan keamanan siber dan literasi digital.

TINJAUAN TEORI DAN PENGEMBANGAN HIPOTESIS

Konsep Budaya Keamanan Siber & Dimensinya

Budaya keamanan siber (*cybersecurity culture*) secara umum dipahami sebagai kumpulan nilai, sikap, norma, dan perilaku yang dimiliki bersama dalam suatu organisasi terkait bagaimana informasi dan sistem digital dilindungi dari ancaman siber. Misalnya, dalam studi Reconceptualizing cybersecurity awareness capability in the data-driven digital economy [3] ditemukan bahwa kemampuan organisasi dalam "cybersecurity awareness" mencakup tiga aspek: personel (pengetahuan, sikap, pembelajaran), manajemen (pelatihan, budaya, orientasi strategis), dan infrastruktur (teknologi dan tata kelola data). Dari sini muncul bahwa dimensi seperti kesadaran keamanan (*awareness*), perilaku keamanan (*behavior*), dukungan manajemen & pelatihan (*management support/training*) adalah bagian penting dari budaya keamanan siber.

Keterkaitan Kesadaran dan Perilaku Keamanan

Kesadaran keamanan merupakan dasar dari budaya keamanan siber karena tanpa pemahaman akan risiko dan ancaman, sulit bagi karyawan untuk memperlihatkan perilaku yang aman. Sebagai contoh, Akter et al. (2022) menegaskan bahwa kurangnya "cybersecurity awareness" membuka kelemahan besar dalam menghadapi ancaman data di era ekonomi digital. Dalam penelitian di Indonesia, Cybersecurity Compliance and Other Factors Influencing Employee Protective Behavior: A Case Study of Bank X in Indonesia (2024) menemukan bahwa program kebijakan, pelatihan (SETA) dan awareness secara signifikan mempengaruhi perilaku protektif karyawan dalam sektor perbankan. Hubungan antara perilaku keamanan (security behavior) dan hasil organisasi juga ditemukan dalam kajian terbaru. Meskipun spesifik organisasi berbeda, logikanya berlaku: perilaku keamanan yang baik menyebabkan risiko insiden menurun sehingga keandalan sistem meningkat.

Kepatuhan Kebijakan & Dukungan Manajemen & Pelatihan

Kepatuhan terhadap kebijakan keamanan (*policy compliance*) dan dukungan manajemen & pelatihan (*management support & training*) kerap disebut sebagai faktor struktural-organisasi yang memfasilitasi budaya keamanan siber. Misalnya, studi Bank X (2024) di atas menunjukkan bahwa kebijakan dan pelatihan meningkatkan awareness kemudian menjadi basis bagi sikap dan perilaku keamanan. Namun, beberapa literatur juga mencatat

DOI: https://doi.org/10.31004/riggs.v5i2.12720

bahwa kepatuhan formal saja belum menjamin peningkatan performa; karena internalisasi nilai dan motivasi individu juga penting untuk menyalurkan kepatuhan ke dalam kinerja nyata.

Literasi Digital sebagai Variabel Moderasi

Peran literasi digital (*digital literacy*) dapat diartikan sebagai kemampuan individu untuk memahami, mengakses, mengevaluasi, dan menggunakan teknologi digital secara efektif dan aman di lingkungan kerja. Misalnya, studi Enhancing Remote Work Satisfaction and Performance based on Information and Digital Literacy (2023) menunjukkan bahwa literasi digital dan literasi informasi memiliki efek positif terhadap kinerja pekerja jarak jauh [4]. Artikel lain seperti Hey Leaders, It's Time to Train the Workforce: Critical Skills in the Digital Workplace (2023) mengidentifikasi literasi digital sebagai salah satu dari sembilan keterampilan kritis di lingkungan kerja digital. Dengan demikian, literasi digital dapat memainkan peran moderasi: yaitu memperkuat (atau dalam kondisi tertentu, melemahkan) pengaruh budaya keamanan siber terhadap kinerja karyawan, karena ketika individu memiliki literasi digital tinggi, mereka akan lebih mampu menerjemahkan awareness, compliance, dan behavior menjadi hasil kinerja yang nyata.

Bukti Moderasi Literasi Digital

Walau masih terbatas, literatur terbaru mulai mengeksplorasi literasi digital dalam peran moderasi atau mediator. Sebagai contoh, studi nasional di Indonesia yang menguji hubungan budaya organisasi, literasi digital, dan kinerja karyawan menemukan bahwa literasi digital memiliki pengaruh langsung terhadap kinerja, meskipun dalam model tersebut bukan sebagai moderasi langsung tetapi sebagai variabel tambahan [5]. Studi-terkini menyiratkan bahwa literasi digital yang tinggi dapat "membuka jalan" bagi efektivitas budaya keamanan siber; sedangkan literasi rendah mungkin menyebabkan gap antara kebijakan/awareness dan tindakan nyata.

Kinerja Karyawan

Kinerja karyawan (*employee performance*) dalam konteks organisasi digital tidak hanya mencakup aspek tradisional (efisiensi, efektivitas, kepatuhan terhadap tugas) tetapi juga adaptasi teknologi, keandalan dalam operasi digital, dan kualitas layanan berbasis digital. Kajian seperti Digital Skills To Improve Work Performance (2024) menyoroti bahwa keterampilan digital berkorelasi positif dengan kinerja kerja dalam industri manufaktur [6]. Dalam transportasi publik digital, karyawan yang mampu memanfaatkan sistem digital dengan aman dan efisien berharap memiliki kinerja lebih baik (tepat waktu, akurat, aman) dibanding yang belum.

Pengaruh Budaya Keamanan Siber terhadap Kinerja

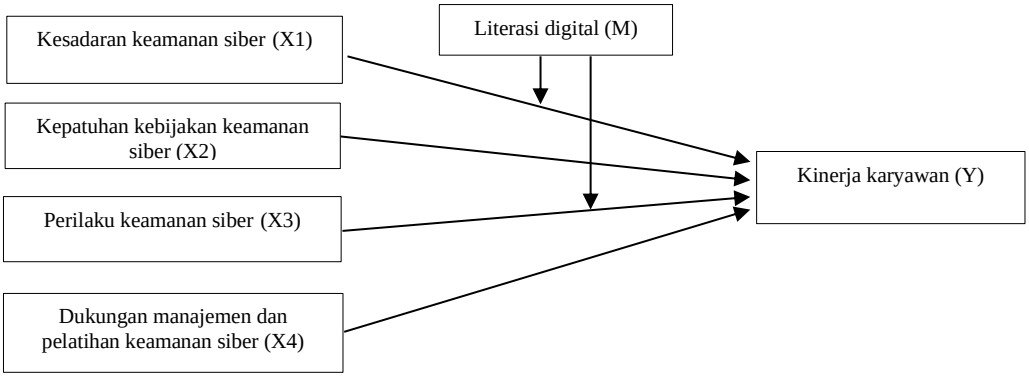
Berdasarkan literatur, beberapa hubungan empiris dapat dikemukakan:

- Kesadaran keamanan mempengaruhi kinerja, bahwa karyawan yang paham risiko siber akan lebih siap menghadapi gangguan sistem, sehingga pelayanan berjalan mulus.
- Perilaku keamanan mempengaruhi kinerja, bahwa segala tindakan yang mengindikasikan rasa aman (misalnya menggunakan password kuat, tidak mengakses situs berbahaya) akan mengurangi downtime dan error serta meningkatkan reliabilitas kinerja.
- Dukungan manajemen & pelatihan terhadap kinerja, dapat dinyatakan bahwa organisasi yang secara aktif akan mendukung keamanan siber dan melatih karyawan menciptakan kondisi kerja yang lebih baik sehingga karyawan lebih produktif.
- Kepatuhan kebijakan mempengaruhi kinerja, meskipun logis bahwa kepatuhan meningkatkan kinerja, banyak hasil penelitian menunjukkan bahwa hasil empiris terkadang lemah atau tidak signifikan karena kepatuhan formal tidak selalu diterjemahkan ke dalam perilaku dan hasil nyata.

Studi-terkini mendukung beberapa poin di atas. Misalnya, dalam sektor publik di Indonesia, penelitian tentang digital culture (yang mirip dengan budaya keamanan siber dalam aspek perilaku digital) menunjukkan bahwa budaya digital yang baik berpengaruh positif terhadap kinerja karyawan. Namun, ada juga hasil yang menunjukkan bahwa pengaruh budaya digital tidak selalu signifikan atau langsung ke kinerja; faktor lain seperti literasi, teknologi, lingkungan kerja turut memengaruhi.

DOI: https://doi.org/10.31004/riggs.v5i2.12720

Kerangka konseptual



Gambar 1 Kerangka Konseptual

Hipotesis Penelitian

Berdasarkan latar belakang masalah, kajian teori dan kerangka konseptual maka hipotesis yang diajukan dalam penelitian sebagai berikut.

1. Diduga kesadaran keamanan siber (X1) berpengaruh positif dan signifikan terhadap kinerja karyawan (Y)
2. Diduga kepatuhan kebijakan keamanan siber (X2) berpengaruh positif dan signifikan terhadap kinerja karyawan (Y)
3. Diduga perilaku keamanan siber (X3) berpengaruh positif dan signifikan terhadap kinerja karyawan (Y)
4. Diduga dukungan manajemen dan pelatihan keamanan siber (X4) berpengaruh positif dan signifikan terhadap kinerja karyawan (Y)
5. Diduga literasi digital (M) memoderasi pengaruh kesadaran keamanan siber (X1) terhadap kinerja karyawan (Y)
6. Diduga literasi digital (M) memoderasi pengaruh perilaku keamanan siber (X3) terhadap kinerja karyawan (Y)

2. Research Methods

Penelitian ini menggunakan desain kuantitatif dengan pendekatan survei korelasional. Tujuannya untuk menguji pengaruh Kesadaran Keamanan Siber (X) terhadap Kinerja Karyawan (Y) serta melihat peran Literasi Digital (M) sebagai variabel moderasi. Data dikumpulkan melalui kuesioner berbasis skala Likert 1–5, untuk menilai persepsi karyawan terhadap dimensi budaya keamanan siber, literasi digital, dan kinerja kerja. Analisis data dilakukan menggunakan Moderating Regression Analysis (MRA).

Populasi penelitian adalah seluruh karyawan Suroboyo Bus yang terlibat langsung dalam operasional dan penggunaan sistem transportasi digital yang berjumlah 180 karyawan termasuk: Staf operator sistem tiket elektronik dan pembayaran non-tunai; Staf layanan pelanggan dan frontliner digital; Driver dan kondektur yang menggunakan aplikasi dalam operasional; dan Staf administrasi dan teknis IT (pengelola data & aplikasi). Populasi sudah teridentifikasi dan relatif terbatas, teknik yang digunakan *simple random sampling*, apabila setiap karyawan memiliki peluang yang sama untuk terpilih dan akses ke semua responden relatif mudah. *Proportionate Stratified Random Sampling*, jika peneliti ingin memastikan keterwakilan tiap divisi atau jabatan sesuai proporsinya. Ukuran sampel dihitung menggunakan rumus Slovin untuk populasi terbatas dengan tingkat kesalahan (*margin of error*) 5% [7].

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

Dimana:

n= ukuran sampel
N= jumlah populasi
e= margin of error (0,05)

DOI: https://doi.org/10.31004/riggs.v5i2.12720

Maka ukuran sampel dapat dikalkulasi sebagai berikut:

$$n = \frac{180}{1 + 180(0{,}05)^2} = \frac{180}{1 + 180(0{,}0025)} = \frac{180}{1 + 0{,}45} = \frac{180}{1{,}45} \approx 124$$

Jumlah sampel dalam studi ini adalah **±124 responden**, yang cukup representatif untuk analisis MRA.

Variabel-variabel yang diteliti didefinisikan secara operasional untuk merefleksikan informasi data melalui indikator yang mengacu pada beberapa penelitian terdahulu. Untuk lebih jelasnya disajikan pada tabel berikut.

Tabel 1 Definisi Operasional Variabel dan Indikator Variabel

Variabel	Definisi Operasional	Indikator
X_1 – Kesadaran Keamanan (*Security Awareness*)	Tingkat pemahaman dan kewaspadaan karyawan terhadap risiko keamanan siber yang terkait dengan penggunaan sistem digital.	1. Mengetahui potensi risiko keamanan siber di lingkungan kerja. 2. Mampu mengenali email/phishing yang mencurigakan. 3. Memahami pentingnya proteksi data pribadi dan perusahaan. 4. Mampu mengidentifikasi potensi ancaman digital.
X_2 – Kepatuhan Kebijakan (Policy Compliance)	Tingkat kepatuhan karyawan terhadap aturan dan prosedur keamanan siber perusahaan.	1. Mematuhi prosedur login dan logout sistem digital. 2. Mengikuti pedoman penggunaan password yang aman. 3. Mematuhi aturan akses data sensitif. 4. Melaporkan insiden keamanan sesuai SOP.
X_3 – Perilaku Keamanan (Security Behavior)	Tindakan nyata yang dilakukan karyawan untuk menjaga keamanan sistem dan data digital dalam pekerjaan sehari-hari.	1. Mengganti password secara berkala 2. Menyimpan dokumen sensitif dengan aman. 3. Menggunakan perangkat lunak keamanan yang disediakan. 4. Menghindari penggunaan perangkat pribadi untuk sistem kerja.
X_4 – Dukungan Manajemen & Pelatihan (Management Support & Training)	Tingkat dukungan organisasi dan pelatihan yang diberikan untuk meningkatkan budaya keamanan siber karyawan.	1. Ketersediaan pelatihan keamanan siber rutin. 2. Pemberian panduan SOP keamanan digital. 3. Adanya monitoring dan feedback manajemen. 4. Motivasi dan reward terkait kepatuhan keamanan.
Y – Kinerja Karyawan (Employee Performance)	Tingkat efektivitas dan efisiensi karyawan dalam menjalankan tugas operasional berbasis sistem digital.	1. Produktivitas operasional harian. 2. Ketepatan penggunaan sistem digital. 3. Minimnya kesalahan operasional terkait sistem. 4. Respons cepat terhadap masalah sistem.
M – Literasi Digital (Digital Literacy)	Kemampuan karyawan memahami, menggunakan, dan memanfaatkan teknologi digital secara efektif untuk mendukung pekerjaan.	1. Menguasai penggunaan aplikasi dan sistem digital internal. 2. Memahami fitur keamanan dalam sistem digital. 3. Cepat menyesuaikan diri dengan update sistem. 4. Mengoptimalkan teknologi untuk efisiensi kerja.

Data penelitian ini diperoleh melalui kuesioner tertutup yang disusun berdasarkan indikator operasional variabel Budaya Keamanan Siber, Literasi Digital, dan Kinerja Karyawan. Setiap item diukur menggunakan skala Likert 1–5 (1 = Sangat Tidak Setuju, 5 = Sangat Setuju). Kuesioner dibagikan secara langsung (offline) kepada karyawan Suroboyo Bus yang menjadi responden, serta dilengkapi versi daring (Google Form) untuk memudahkan pengumpulan data. Sebelum penyebaran penuh, dilakukan uji coba (pilot test) pada sekitar 20 responden untuk menilai validitas isi dan reliabilitas awal instrumen. Hasil uji validitas dan reliabilitas akhir (menggunakan Cronbach's Alpha dan Corrected Item-Total Correlation) memastikan bahwa setiap item memenuhi syarat ≥ 0,70 untuk reliabilitas dan ≥ 0,30 untuk validitas.

DOI: https://doi.org/10.31004/riggs.v5i2.12720

Analisis data dilakukan secara kuantitatif menggunakan bantuan program SPSS dengan langkah-langkah berikut: Uji Validitas dan Reliabilitas; uji normalitas, multikolinearitas, heteroskedastisitas, dan autokorelasi agar model regresi memenuhi syarat BLUE (Best Linear Unbiased Estimator); Analisis Regresi Linier Berganda; Moderated Regression Analysis (MRA).

3. Results and Discussions

Karakteristik Responden

Responden dalam penelitian ini adalah karyawan aktif Suroboyo Bus yang terlibat langsung dalam operasional dan sistem transportasi digital. Mereka terdiri atas berbagai jabatan yang berhubungan dengan penggunaan aplikasi tiket elektronik, sistem pembayaran non-tunai, serta sistem administrasi digital. Berikut karakteristik yang digunakan dalam penelitian.

Jenis Kelamin

Klasifikasi gender penting untuk melihat persebaran partisipasi dan potensi perbedaan persepsi terhadap keamanan siber. Laki-laki, umumnya mendominasi posisi driver, petugas lapangan, dan staf teknis. Perempuan, lebih banyak di posisi frontliner, layanan pelanggan, dan administrasi.

Tabel 2 Distribusi Frekuensi Responden Berdasarkan Jenis Kelamin

Jenis Kelamin	Jumlah	Persentase
Laki-laki	85	68,5%
Perempuan	39	31,5%
Total	124	100%

Sumber: Data diolah, 2026

Usia Responden

Variabel usia mencerminkan tingkat kematangan kerja dan kesiapan adaptasi digital. Kategori: <25 tahun → generasi muda, relatif cepat adaptasi digital; 26–35 tahun → usia produktif dominan di sistem transportasi publik; 36–45 tahun → berpengalaman namun cenderung hati-hati dalam teknologi baru, dan > 45 tahun → posisi senior atau pengawas.

Tabel 3 Hasil Distribusi Frekuensi Responden Berdasarkan Usia

Usia (Tahun)	Jumlah	Persentase
<25	18	14,5%
26–35	59	47,6%
36–45	33	26,6%
>45	14	11,3%
Total	124	100%

Sumber: Data diolah, 2026

Tingkat Pendidikan Terakhir

Tingkat pendidikan menggambarkan kompetensi dasar dan kemampuan memahami pelatihan keamanan siber maupun teknologi digital. Kategori umum: SMA/SMK → mayoritas driver, kondektur, dan petugas lapangan; Diploma (D3) → staf administrasi, frontliner digital; S1 → staf manajemen dan teknis IT.

Tabel 4 Hasil Distribusi Frekuensi Responden Berdasarkan Tingkat Pendidikan

Pendidikan	Jumlah	Persentase
SMA/SMK	58	46,8%
D3	37	29,8%
S1	29	23,4%
Total	124	100%

Sumber: Data diolah, 2026

DOI: https://doi.org/10.31004/riggs.v5i2.12720

Jabatan/ Posisi Kerja

Posisi kerja menunjukkan tingkat keterlibatan responden dengan sistem digital, yang dapat mempengaruhi persepsi terhadap budaya keamanan siber.

Tabel 5 Hasil Distribusi Frekuensi Responden Berdasarkan Jabatan

Jabatan/Posisi	Deskripsi Peran	Jumlah	Persentase
Driver	Mengoperasikan armada dengan aplikasi tiket digital dan sistem navigasi	41	33,1%
Kondektur/ Petugas Tiket	Mengelola transaksi non-tunai & aplikasi tiket digital	28	22,6%
Staf Layanan Pelanggan/ Frontliner	Melayani pelanggan dan menggunakan aplikasi layanan digital	22	17,7%
Staf Administrasi & Keuangan	Menginput dan mengelola data operasional berbasis sistem digital	18	14,5%
Staf IT & Teknis Sistem	Mengelola server, data, dan aplikasi digital operasional	15	12,1%
Total		124	100%

Sumber: Data diolah, 2026

Masa Kerja

Lama masa kerja menggambarkan tingkat pengalaman dan paparan terhadap kebijakan keamanan siber perusahaan.

Tabel 6 Hasil Distribusi Frekuensi Responden Berdasarkan Masa Kerja

Lama Bekerja	Jumlah	Persentase
<1 tahun	9	7,3%
1–3 tahun	38	30,6%
4–6 tahun	54	43,5%
>6 tahun	23	18,6%
Total	124	100%

Sumber: Data diolah, 2026

Berdasarkan data karakteristik responden di atas dapat diinterpretasikan bahwa Komposisi responden menunjukkan dominasi usia produktif (26–35 tahun) dengan pendidikan menengah ke atas, menandakan kesiapan cukup tinggi dalam penerapan budaya keamanan siber, proporsi gender memperlihatkan dominasi laki-laki yang umum pada sektor transportasi publik, dan sebagian besar responden memiliki masa kerja lebih dari 3 tahun, sehingga sudah mengenal prosedur dan sistem digital di Suroboyo Bus.

Hasil Pengujian MRA (Moderating Regression Analisis)

Tabel 7 Hasil Analisis Multiple Regrestion

Variabel Independen	Beta (β)	t hitung	Sig.	Keterangan
Kesadaran Keamanan (X_1)	0,278	3,842	0,000	Signifikan
Kepatuhan Kebijakan (X_2)	0,231	3,107	0,002	Signifikan
Perilaku Keamanan (X_3)	0,087	1,287	0,201	Tidak signifikan
Dukungan Manajemen & Pelatihan (X_4)	0,321	4,214	0,000	Signifikan

Sumber: Data diolah, 2026

Hasil nilai $R^2 = 0,612$ artinya 61,2% variasi kinerja karyawan dijelaskan oleh empat dimensi budaya keamanan siber. Adjusted $R^2 = 0,595$ F hitung = 36,48; Sig. = 0,000 → model regresi signifikan secara simultan. Hasil

DOI: https://doi.org/10.31004/riggs.v5i2.12720

tersebut dapat diinterpretasikan bahwa tiga dimensi budaya keamanan siber yaitu (kesadaran keamanan, kepatuhan kebijakan, dan dukungan manajemen) berpengaruh positif dan signifikan terhadap kinerja karyawan. Sedangkan perilaku keamanan siber tidak berpengaruh signifikan, kemungkinan karena perilaku tersebut sudah dianggap sebagai rutinitas kerja, bukan faktor pendorong kinerja secara langsung.

Analisis Moderated Regression (MRA)

Variabel moderasi: Literasi Digital (M). Langkah MRA dilakukan dengan menambahkan variabel interaksi (X × M) untuk dua hubungan yang relevan (sesuai kesepakatan awal: hanya dua X dimoderasi).

Tabel 8 Hasil Analisis MRA

Variabel	Beta (β)	t hitung	Sig.	Keterangan
Literasi Digital (M)	0,247	3,216	0,002	Signifikan
X_1 × M (Kesadaran Keamanan × Literasi Digital)	0,196	2,765	0,007	Signifikan
X_2 × M (Kepatuhan Kebijakan × Literasi Digital)	0,041	0,683	0,496	Tidak signifikan

Sumber: Data diolah, 2026

R^2 Model Moderasi = 0,687, meningkat dari 0,612 (tanpa moderasi) → ada peningkatan 7,5% setelah memasukkan variabel literasi digital. F hitung = 42,81; Sig. = 0,000. Berdasarkan hasil Analisa di atas dapat diinterpretasi bahwa: Literasi digital memoderasi pengaruh kesadaran keamanan terhadap kinerja karyawan secara positif dan signifikan. Artinya, semakin tinggi literasi digital, semakin kuat hubungan antara kesadaran keamanan siber dan kinerja. Namun, literasi digital tidak memoderasi hubungan antara kepatuhan kebijakan dengan kinerja karyawan; artinya tingkat literasi digital tidak memperkuat efek kepatuhan terhadap hasil kerja.

Hasil Pengujian Hipotesis

Berdasarkan hasil perhitungan SPSS sebagaimana telah dijelaskan di atas maka hasil pengujian hipotesis dapat disajikan pada tabel berikut:

Tabel 9 Ringkasan Hasil Pengujian Hipotesis

Hipotesis	Pernyataan Hipotesis	Hasil	Keterangan
H1	Kesadaran Keamanan (X_1) → Kinerja Karyawan (Y)	β = 0,278; Sig. 0,000	Diterima
H2	Kepatuhan Kebijakan (X_2) → Kinerja Karyawan (Y)	β = 0,231; Sig. 0,002	Diterima
H3	Perilaku Keamanan (X_3) → Kinerja Karyawan (Y)	β = 0,087; Sig. 0,201	Ditolak
H4	Dukungan Manajemen & Pelatihan (X_4) → Kinerja Karyawan (Y)	β = 0,321; Sig. 0,000	Diterima
H5	Literasi Digital memoderasi (X_1 → Y)	β = 0,196; Sig. 0,007	Diterima
H6	Literasi Digital memoderasi (X_2 → Y)	β = 0,041; Sig. 0,496	Ditolak

Sumber: Data diolah, 2026

X_4 – Dukungan Manajemen & Pelatihan (β=0,321) → tinggi. Artinya, dimensi ini paling berpengaruh terhadap kinerja karyawan. Secara empiris, dukungan pimpinan dan pelatihan rutin memperkuat kesadaran karyawan terhadap keamanan siber dan kemampuan digital mereka, sehingga berimbas langsung pada produktivitas kerja. X_1 – Kesadaran Keamanan (β=0,278) → sedang. Karyawan yang sadar akan risiko keamanan digital cenderung lebih berhati-hati dan mematuhi SOP digital, sehingga berpengaruh sedang terhadap kinerja. X_2 – Kepatuhan Kebijakan (β=0,231) → sedang. Kepatuhan terhadap aturan formal perusahaan berkontribusi pada kinerja, namun efeknya tidak setinggi dukungan manajemen, kemungkinan karena kepatuhan formal lebih bersifat pasif dibandingkan praktik langsung yang dibimbing pimpinan. X_3 – Perilaku Keamanan (β=0,087) → rendah/sangat kecil. Nilai beta yang kecil dan tidak signifikan menunjukkan bahwa perilaku keamanan sehari-hari tidak secara langsung meningkatkan kinerja. Secara empiris, perilaku ini mungkin sudah menjadi rutinitas yang diterapkan oleh semua karyawan sehingga variabilitasnya rendah.

DOI: https://doi.org/10.31004/riggs.v5i2.12720

H1, H2, H4 diterima karena dimensi budaya keamanan siber yang terkait dengan kesadaran, kepatuhan, dan dukungan manajemen memiliki peran nyata dalam meningkatkan kinerja. Dukungan manajerial dan pelatihan memberi bimbingan langsung yang mendorong produktivitas, sedangkan kesadaran dan kepatuhan menciptakan perilaku kerja yang konsisten dan aman. H3 ditolak, perilaku keamanan sehari-hari tidak signifikan terhadap kinerja karena dianggap sudah menjadi kebiasaan rutin; perbedaan perilaku antar karyawan tidak cukup besar untuk mempengaruhi output kinerja secara statistik.

Analisis moderasi literasi digital nilai beta (β) diinterpretasi sebagai berikut:

a. $X_1 \times M$ (β=0,196) sedang. Literasi digital memperkuat pengaruh kesadaran keamanan terhadap kinerja. Artinya, karyawan yang paham literasi digital mampu menerapkan kesadaran keamanan lebih efektif, sehingga berdampak nyata pada produktivitas,

b. $X_2 \times M$ (β=0,041) sangat kecil / tidak signifikan. Literasi digital tidak memperkuat pengaruh kepatuhan kebijakan terhadap kinerja, kemungkinan karena kepatuhan terhadap aturan formal bersifat prosedural, tidak tergantung kemampuan digital yang lebih tinggi.

c. H5 diterima literasi digital relevan dalam meningkatkan efektivitas kesadaran keamanan, karena karyawan yang mahir teknologi cenderung lebih cepat mengenali potensi risiko dan mengambil tindakan pencegahan.
d. H6 ditolak literasi digital tidak mengubah dampak kepatuhan kebijakan terhadap kinerja, karena kepatuhan lebih mengacu pada disiplin mengikuti aturan, bukan pada kemampuan digital individu.

Pembahasan Hasil Penelitian

Pengaruh Budaya Keamanan Siber terhadap Kinerja Karyawan

Hasil penelitian menunjukkan bahwa dukungan manajemen & pelatihan (X_4) memiliki pengaruh paling besar terhadap kinerja karyawan (β=0,321, p<0,001), diikuti kesadaran keamanan (X_1) dan kepatuhan kebijakan (X_2). Sebaliknya, perilaku keamanan (X_3) tidak berpengaruh signifikan. Interpretasi teoritis, bahwa (1) dukungan manajemen dan pelatihan sesuai dengan teori Organizational Support Theory yang menyatakan bahwa karyawan akan menunjukkan kinerja optimal ketika mereka menerima dukungan dari organisasi [8] [9]. (2) Kesadaran keamanan meningkatkan kewaspadaan karyawan terhadap risiko siber, yang secara langsung berdampak pada kelancaran operasional dan efisiensi kerja. Penelitian terbaru di sektor transportasi digital menunjukkan tren serupa: karyawan yang sadar risiko keamanan digital mampu mengurangi kesalahan operasional dan gangguan sistem. (3) Kepatuhan kebijakan juga memengaruhi kinerja, namun lebih moderat. Secara empiris, kepatuhan formal cenderung pasif dan prosedural; karyawan mematuhi aturan tetapi tidak selalu aktif meningkatkan produktivitas. (4) Perilaku keamanan yang tidak signifikan menunjukkan adanya efek ceiling: hampir semua karyawan sudah memiliki rutinitas keamanan yang stabil, sehingga variabilitasnya kecil dan dampaknya terhadap kinerja tidak terdeteksi secara statistik. Maka budaya keamanan siber secara umum penting bagi kinerja, namun aspek yang memberikan bimbingan aktif dan dukungan organisasi lebih berpengaruh daripada perilaku individu yang rutin.

Moderasi Literasi Digital

Hasil MRA menunjukkan bahwa literasi digital memoderasi hubungan kesadaran keamanan → kinerja (β=0,196, p=0,007), tetapi tidak signifikan pada hubungan kepatuhan kebijakan → kinerja (β=0,041, p=0,496). Interpretasi teoritis, bahwa literasi digital meningkatkan kemampuan karyawan dalam menerapkan kesadaran keamanan siber secara efektif. Karyawan yang paham teknologi dapat mendeteksi risiko lebih cepat, menyesuaikan diri dengan sistem digital, dan mengoptimalkan penggunaan aplikasi operasional. Hal ini sejalan dengan temuan sebelumnya bahwa literasi digital memperkuat efektivitas kesadaran keamanan dalam sektor transportasi publik digital. Literasi digital tidak memoderasi kepatuhan kebijakan karena kepatuhan lebih bersifat formal dan prosedural. Karyawan tetap mengikuti aturan, terlepas dari kemampuan digital mereka. Penelitian sejenis [10] menegaskan bahwa kepatuhan formal bersifat mandatory sehingga literasi digital tidak memberikan dampak tambahan signifikan. Dengan demikian moderasi literasi digital menegaskan bahwa faktor kemampuan kognitif digital menjadi kunci dalam mengoptimalkan efek budaya keamanan siber terhadap kinerja, khususnya pada aspek kesadaran risiko.

DOI: https://doi.org/10.31004/riggs.v5i2.12720

Penelitian ini memperkuat teori Organizational Support Theory dan Information Security Culture dalam konteks transportasi publik digital. Dukungan manajemen dan pelatihan terbukti paling berpengaruh terhadap kinerja, menegaskan bahwa bimbingan organisasi lebih penting daripada perilaku individu rutin. Menunjukkan peran literasi digital sebagai moderator selektif: literasi digital meningkatkan efektivitas kesadaran keamanan, tetapi tidak memoderasi pengaruh kepatuhan kebijakan. Temuan ini memberikan kontribusi teoretis baru terkait interaksi kemampuan digital dan budaya keamanan siber dalam organisasi transportasi. Penelitian menyoroti variabilitas pengaruh dimensi budaya keamanan siber, menandakan bahwa dimensi yang bersifat aktif dan didukung organisasi lebih menentukan kinerja daripada dimensi yang bersifat rutin/prosedural.

4. Conclusion

Budaya keamanan siber berpengaruh signifikan terhadap kinerja karyawan Suroboyo Bus, terutama pada dimensi dukungan manajemen & pelatihan, kesadaran keamanan, dan kepatuhan kebijakan. Perilaku keamanan tidak berpengaruh signifikan karena dianggap sudah menjadi kebiasaan rutin. Literasi digital memoderasi hubungan kesadaran keamanan → kinerja, namun tidak pada hubungan kepatuhan kebijakan → kinerja. Secara keseluruhan, kombinasi dukungan manajemen, pelatihan, kesadaran keamanan, dan literasi digital menjadi kunci dalam meningkatkan kinerja karyawan pada sistem transportasi publik digital. Saran penelitian untuk praktisi: Tingkatkan program pelatihan berbasis praktik nyata, bukan hanya teori; Fokus pada peningkatan literasi digital karyawan, khususnya untuk frontliner dan operator sistem digital; dan Kombinasikan kebijakan formal dengan monitoring berbasis teknologi untuk meningkatkan efektivitas kepatuhan. Manajemen Organisasi: Pimpinan Suroboyo Bus sebaiknya fokus pada dukungan manajemen dan pelatihan rutin untuk meningkatkan kinerja karyawan dalam penggunaan sistem digital. Pelatihan Literasi Digital: Program edukasi digital diperlukan agar kesadaran keamanan siber diterjemahkan ke tindakan nyata, terutama untuk staf operasional dan frontliner digital. Efektivitas Kepatuhan: Meskipun kepatuhan kebijakan penting, organisasi perlu memadukannya dengan praktik aktif (misalnya simulasi risiko dan pengawasan rutin) untuk meningkatkan kinerja nyata. Automasi dan Monitoring: Perilaku keamanan rutin bisa didukung dengan teknologi monitoring untuk mencegah human error dan meningkatkan keamanan sistem digital. Saran untuk peneliti selanjutnya: Lakukan penelitian longitudinal untuk melihat perubahan budaya keamanan siber dan literasi digital dari waktu ke waktu; Uji variabel moderasi tambahan, seperti motivasi, pengalaman kerja, atau budaya organisasi; dan Luaskan populasi ke sektor transportasi digital lainnya untuk generalisasi temuan.

Reference

[1] A. Hendriawan, I. Gautama, D. Siahaan, and K. Kurniawan, "Analysis of The Influence of Factors on Maritime Cyber Resilience on Board With Intervening Maritime Cyber Security Awareness," *Syntax Lit. ; J. Ilm. Indones.*, vol. 10, no. 3, pp. 2783–2794, 2025, doi: 10.36418/syntax-literate.v10i3.56311.

[2] D. Samudra, Tamamudin, and Ayatullah, "Innovation Digital Literacy Public Administration in Indonesia: National Survey Data," *Citiz. J. Ilm. Multidisiplin Indones.*, vol. 5, no. 2, pp. 560–565, 2025, doi: 10.53866/jimi.v5i2.757.

[3] S. Akter, R. Bandara, U. Hani, S. F. Wamba, C. Foropon, and T. Papadopoulos, "Reconceptualizing Cybersecurity Awareness Capability in The Data-Driven Digital Economy," *Ann. Oper. Res.*, 2022, doi: https://doi.org/10.1007/s10479-022-04844-8.

[4] M. Sholikah and A. Safitri, "Enhancing Remote Work Satisfaction and Performance based on Information and Digital Literacy," *J. Off. Adm. Educ. Pract.*, vol. 5, no. 1, pp. 36–43, 2025, doi: 10.26740/joaep.v5n1.p36-43.

[5] R. Dessa, R. Hidayat, and E. S. Mubarok, "Influence of organizational culture, work-life balance, and digital literacy on employee performance," *J. Multidisiplin Sahombu*, vol. 5, no. 05, pp. 1287–1304, 2025, doi: 10.58471/jms.v5i05.

[6] M. Sartika, S. D. Astuti, A. N. Chasanah, and F. Riyanto, "Digital Skills To Improve Work Performance," *Int. J. Accounting, Manag. Econ. Res.*, vol. 1, no. 2, pp. 33–40, 2023, doi: 10.56696/ijamer.v1i2.14.

[7] S. Bahri, *Metodologi Penelitian Bisnis - Lengkap Dengan Teknik Pengolahan Data SPSS*, 2nd ed. Penerbit Andi, Yogyakarta, 2025.

[8] L. Rhoades and R. Eisenberger, "Perceived Organizational Support: A Review of the Literature," *J. Appl. Psychol.*, vol. 87, no. 4, pp. 698–714, 2002, doi: https://doi.org/10.1037/0021-9010.87.4.698.

[9] J. N. Kurtessis, R. Eisenberger, L. C. Ford, M. T., Buffardi, K. A. Stewart, and C. S. Adis, "Perceived Organizational Support: A Meta-Analytic Evaluation of Organizational Support Theory," *J. Manage.*, vol. 43, no. 6, pp. 1854–1884, 2017.

[10] A. Hama, "Analisis Kesadaran Pajak dan Efektivitas E-Filing Terhadap Kepatuhan Wajib Pajak dengan Literasi Digital Sebagai Variabel Moderasi," *COMSERVA J. Penelit. dan Pengabdi. Masy.*, vol. 2, no. 09, pp. 1783–1794, 2023, doi: 10.59141/comserva.v2i09.556.

DOI: https://doi.org/10.31004/riggs.v5i2.12720