E-ISSN : 2988-1986
https://ejournal.cahayailmubangsa.institute/index.php/kohesi

Kohesi: Jurnal Multidisiplin Saintek
Volume 8 No 11 Tahun 2025

Analisis Risiko Keamanan Siber pada Infrastruktur Digital UMKM di Balikpapan dan Strategi Mitigasi Berbasis Kerangka Kerja Keamanan Siber Nasional

Muhammad Bilal Arroji[1*], Alya Aura Rauf [2], Lalita Desi Talia [3] , Yustian Servanda [4] , Pramudya Prima Insan [5]
[1,2,3,4,5]Program Studi Sistem informasi , Fakultas Ilmu Komputer, Universitas Mulia Balikpapan
E-mail: info@universitasmulia.ac.id

ABSTRACT

Micro, Small, and Medium Enterprises (MSMEs) in Balikpapan are facing increasing cybersecurity threats as they adopt digital technologies in their operations. This study aims to identify the types and levels of cyber risks faced by MSMEs and to formulate mitigation strategies based on the National Cybersecurity Framework (KKSN) issued by the Indonesian National Cyber and Crypto Agency (BSSN). The research employed a descriptive qualitative approach through interviews, observations, and questionnaires. Risk analysis was conducted using the OCTAVE Allegro model, which allows the identification of critical assets, potential threats, vulnerabilities, and organizational impacts. The findings indicate that most MSMEs lack adequate cybersecurity policies and are vulnerable to phishing attacks, malware infections, and insufficient data backup procedures. The proposed mitigation strategies include improving digital literacy, strengthening basic technical protections, and establishing cybersecurity Standard Operating Procedures (SOPs) based on the five pillars of the KKSN: identification, protection, detection, response, and recovery. This research provides practical contributions to the development of community-based cybersecurity policies and local stakeholder collaboration.

Keywords: MSMEs, cybersecurity, OCTAVE Allegro, KKSN, risk mitigation

ABSTRAK

UMKM di Balikpapan menghadapi ancaman keamanan siber yang meningkat seiring adopsi teknologi digital dalam operasional mereka. Studi ini bertujuan untuk mengidentifikasi jenis dan tingkat risiko siber yang dihadapi oleh UMKM serta menyusun strategi mitigasi berdasarkan Kerangka Keamanan Siber Nasional (KKSN) yang dikeluarkan oleh BSSN. Metodologi yang digunakan adalah pendekatan deskriptif kualitatif melalui wawancara, observasi, dan penyebaran kuesioner. Analisis risiko dilakukan menggunakan model OCTAVE Allegro yang memungkinkan identifikasi aset penting, ancaman potensial, kerentanan, serta dampak terhadap organisasi. Hasil penelitian menunjukkan bahwa sebagian besar UMKM belum memiliki kebijakan keamanan siber yang memadai, rentan terhadap serangan phishing, malware, dan kekurangan dalam backup data. Strategi mitigasi yang diusulkan mencakup peningkatan literasi digital, penguatan proteksi teknis dasar, dan pembentukan SOP keamanan siber sesuai dengan lima

Article History
Received: Juli 2025
Reviewed: Juli 2025
Published: Juli 2025

Plagiarism Checker No 235
Prefix DOI : 10.8734/Kohesi.v1i2.365
Copyright : Author
Publish by : Kohesi

pilar utama dalam KKSN: identifikasi, proteksi, deteksi, respons, dan pemulihan. Penelitian ini memberikan kontribusi praktis bagi pengembangan kebijakan keamanan siber berbasis komunitas dan pemangku kepentingan lokal.

Kata kunci: UMKM, keamanan siber, OCTAVE Allegro, KKSN, mitigasi risiko

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi (TIK) dalam satu dekade terakhir telah membawa transformasi besar dalam cara organisasi menjalankan bisnisnya, termasuk di sektor Usaha Mikro, Kecil, dan Menengah (UMKM). Di Indonesia, UMKM merupakan tulang punggung perekonomian dengan kontribusi mencapai lebih dari 60% terhadap Produk Domestik Bruto (PDB) nasional dan menyerap sekitar 97% tenaga kerja (Kementerian Koperasi dan UKM, 2023). Di tengah era digitalisasi, banyak UMKM mulai mengadopsi sistem informasi sederhana seperti aplikasi kasir digital, pemasaran berbasis media sosial, hingga platform e-commerce untuk meningkatkan efisiensi dan menjangkau pasar yang lebih luas.

Namun, akselerasi digitalisasi ini tidak selalu dibarengi dengan pemahaman dan kesiapan pelaku UMKM terhadap aspek keamanan informasi. Berdasarkan laporan BSSN tahun 2022, lebih dari 50% insiden siber di Indonesia menargetkan sektor usaha kecil dan menengah yang belum memiliki sistem keamanan informasi memadai. Kondisi ini menempatkan UMKM pada posisi yang rentan terhadap berbagai ancaman siber, termasuk phishing, ransomware, pencurian data pelanggan, serta eksploitasi sistem aplikasi yang tidak terproteksi.

Kota Balikpapan sebagai salah satu pusat ekonomi di Kalimantan Timur menunjukkan geliat digitalisasi UMKM yang cukup signifikan, terutama pasca pandemi COVID-19. Pelaku usaha mulai memanfaatkan platform daring seperti marketplace, media sosial, dan sistem pembayaran digital dalam menjalankan usahanya. Akan tetapi, berdasarkan observasi awal, sebagian besar pelaku UMKM di Balikpapan belum memahami pentingnya manajemen risiko siber. Tidak sedikit dari mereka menggunakan perangkat lunak bajakan, tidak melakukan backup data secara rutin, dan tidak mengenali ciri-ciri serangan digital yang umum terjadi.

Masalah utama yang dihadapi adalah belum adanya panduan praktis atau kebijakan lokal yang mengatur tentang tata kelola keamanan siber bagi pelaku UMKM, baik dari sisi teknis maupun prosedural. Selain itu, keterbatasan sumber daya manusia dan keuangan juga menjadi hambatan dalam menerapkan sistem keamanan informasi yang memadai. Penelitian ini hadir untuk mengisi kesenjangan tersebut dengan mengkaji tingkat risiko keamanan siber yang

dihadapi oleh UMKM di Balikpapan dan merancang strategi mitigasi berbasis Kerangka Keamanan Siber Nasional (KKSN) yang dikembangkan oleh Badan Siber dan Sandi Negara (BSSN).

Penelitian ini menggunakan pendekatan OCTAVE Allegro sebagai model analisis risiko yang menekankan pada pentingnya identifikasi aset informasi, pemetaan ancaman, serta pemahaman konteks organisasi dalam menilai dampak risiko. Dengan mengadopsi lima pilar utama dalam KKSN, yaitu identifikasi, proteksi, deteksi, respons, dan pemulihan, diharapkan strategi mitigasi yang dihasilkan dapat diimplementasikan secara bertahap dan berkelanjutan oleh pelaku UMKM. Hasil dari penelitian ini diharapkan dapat menjadi rekomendasi strategis bagi pemangku kepentingan lokal, termasuk pemerintah daerah, komunitas bisnis, dan penyedia layanan digital untuk membangun ekosistem UMKM yang tangguh terhadap ancaman siber.

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan deskriptif dengan metode campuran (mixed-method), yaitu menggabungkan pendekatan kualitatif dan kuantitatif untuk memperoleh pemahaman yang komprehensif mengenai tingkat kesiapan dan risiko keamanan siber pada pelaku Usaha Mikro, Kecil, dan Menengah (UMKM) di Kota Balikpapan. Pendekatan kualitatif digunakan untuk menggali lebih dalam persepsi, pengalaman, dan praktik keamanan digital melalui wawancara dan observasi langsung, sementara pendekatan kuantitatif digunakan untuk mengukur secara sistematis variabel-variabel yang diteliti, seperti literasi digital dan kesiapan keamanan siber. Teknik pengumpulan data meliputi observasi lapangan, wawancara semi-terstruktur, serta penyebaran kuesioner tertutup menggunakan skala Likert lima poin yang disusun berdasarkan indikator dari model OCTAVE Allegro dan lima pilar utama dalam Kerangka Keamanan Siber Nasional (KKSN), yaitu identifikasi, proteksi, deteksi, respons, dan pemulihan. Responden dipilih menggunakan teknik purposive sampling dengan kriteria UMKM aktif yang telah menggunakan sistem digital dalam operasional usaha minimal satu tahun. Data yang diperoleh kemudian diuji validitas isinya melalui penilaian ahli, dan diuji reliabilitasnya menggunakan Cronbach’s Alpha. Untuk menganalisis hubungan antarvariabel, dilakukan uji normalitas menggunakan Shapiro–Wilk, dilanjutkan dengan uji korelasi Pearson dan regresi linier sederhana untuk mengukur pengaruh literasi digital terhadap kesiapan keamanan siber. Selanjutnya, skor masing-masing pilar KKSN dikonversi ke bentuk persentase kesiapan dan dikategorikan berdasarkan standar interpretasi untuk mengetahui kesenjangan (gap) implementasi keamanan siber pada UMKM. Hasil dari seluruh proses ini dijadikan dasar untuk penyusunan strategi mitigasi keamanan siber berbasis kerangka kerja nasional yang aplikatif dan relevan dengan konteks lokal UMKM di Balikpapan.

2.1 Uji Validitas Instrumen

Langkah awal adalah memastikan bahwa setiap butir dalam kuesioner benar-benar mengukur apa yang seharusnya diukur. Uji validitas dilakukan dalam dua tahap:

- Validitas isi (content validity): dilakukan dengan meminta penilaian dari para ahli (expert judgment), termasuk dosen bidang sistem informasi, praktisi keamanan siber, dan pelaku UMKM digital. Mereka menilai sejauh mana item kuesioner sesuai dengan konsep lima pilar KKSN dan indikator dalam kerangka OCTAVE Allegro.
- Validitas butir (item validity): dilakukan dengan korelasi Pearson antara skor item dan skor total. Butir dikatakan valid jika r-hitung > r-tabel (pada taraf signifikansi 5%). Ini memastikan setiap item memiliki kontribusi signifikan terhadap konstruk yang diukur.

2.2 Uji Rehabilitas Instrumen

Setelah validitas teruji, dilanjutkan dengan uji reliabilitas untuk mengetahui konsistensi jawaban responden terhadap instrumen. Digunakan metode Cronbach's Alpha untuk menilai sejauh mana item dalam kuesioner memberikan hasil yang konsisten.

- Nilai $\alpha \geq 0,7$ menunjukkan bahwa kuesioner tersebut reliabel dan layak digunakan dalam pengumpulan data lebih lanjut.
- Uji ini penting karena instrumen yang tidak reliabel akan menghasilkan kesimpulan yang bias, meskipun valid secara teoritis.

2.3 Uji Normalitas (Shapiro-Wilk)

Uji normalitas digunakan untuk memastikan bahwa data yang diperoleh (literasi digital dan kesiapan siber) berdistribusi normal. Distribusi normal adalah asumsi dasar dalam pengujian parametrik seperti korelasi dan regresi.

- Shapiro–Wilk dipilih karena lebih akurat untuk ukuran sampel kecil hingga menengah ($n < 50$).
- Apabila nilai signifikansi (p-value) > 0,05, maka data dinyatakan berdistribusi normal dan layak dianalisis lebih lanjut secara parametrik.Uji Mardia ada dua komponen :

2.4 Uji Korelasi Pearson

Setelah asumsi normalitas terpenuhi, dilakukan pengujian hubungan antara literasi digital sebagai variabel bebas dan kesiapan keamanan siber sebagai variabel terikat menggunakan **korelasi Pearson.**

- Koefisien korelasi (r) menunjukkan arah dan kekuatan hubungan (positif/negatif, lemah/kuat).
- Nilai r antara 0,60–0,79 dikategorikan sebagai hubungan kuat.
- Signifikansi hubungan diuji pada taraf α = 0,05. Hasil yang signifikan menandakan bahwa peningkatan literasi digital berkaitan erat dengan kesiapan keamanan siber yang lebih tinggi.

2.5 Uji Regresi Linier Sederhana

Untuk mengukur seberapa besar kontribusi literasi digital dalam memengaruhi kesiapan keamanan siber, digunakan analisis regresi linier sederhana. Model persamaannya ditulis sebagai:

$$y = a + bX + e$$

Y = variabel dependen (kesiapan keamanan siber)

X = variabel independen (literasi digital)

a = konstanta

b = koefisien pengaruh

e = error/residual

Nilai koefisien b menunjukkan seberapa besar perubahan Y untuk setiap satu unit perubahan X. Signifikansi diuji melalui uji-t, sementara nilai R^2 (koefisien determinasi) menunjukkan proporsi varians Y yang dijelaskan oleh X.

2.6 Konversi dan Interprestasi Skor Kesiapan

Setiap skor pada lima pilar KKSN dihitung dengan rerata dari item-item terkait, kemudian dikonversi menjadi bentuk persentase dengan rumus:

$$skor\ persen = \left(\frac{Skor\ Rata - rata}{5}\right) x\ 100\%$$

Kategori interpretatif digunakan untuk memetakan tingkat kesiapan:

< 25% = Sangat Rendah

25–49% = Rendah

50–74% = Sedang

≥ 75% = Tinggi

Klasifikasi ini memungkinkan peneliti untuk melihat secara visual dan numerik area mana yang paling lemah dan memerlukan prioritas mitigasi.

3. HASIL DAN PEMBAHASAN

Bagian ini menyajikan hasil dari pengujian statistik yang dilakukan terhadap data yang diperoleh, serta pembahasan terhadap makna dari temuan tersebut dalam konteks risiko keamanan siber pada UMKM. Pengujian dilakukan secara berurutan mulai dari uji validitas, reliabilitas, normalitas, korelasi, regresi linier, hingga konversi skor KKSN.

3.1 Hasil Uji Validitas dan Reliabilitas

Uji validitas butir kuesioner menunjukkan bahwa seluruh item memiliki nilai r-hitung lebih besar dari r-tabel (0,361 pada α = 0,05), sehingga dinyatakan valid. Hal ini menunjukkan bahwa seluruh indikator dalam kuesioner mampu mengukur dimensi yang diinginkan. Sementara itu, uji reliabilitas dengan Cronbach's Alpha menghasilkan nilai sebesar 0,803, yang berarti bahwa instrumen memiliki tingkat konsistensi internal yang sangat baik dan dapat digunakan dalam skala pengukuran yang lebih luas.

3.2 Hasil Uji Normalitas

Pengujian normalitas dilakukan dengan menggunakan uji Shapiro–Wilk, dengan hasil sebagai berikut:

- Literasi Digital: $p = 0{,}112 > 0{,}05 \rightarrow$ data berdistribusi normal
- Kesiapan Keamanan Siber: $p = 0{,}087 > 0{,}05 \rightarrow$ data berdistribusi normal

Karena kedua variabel menunjukkan nilai signifikansi di atas 0,05, maka dapat disimpulkan bahwa distribusi data bersifat normal dan pengujian statistik parametrik dapat digunakan.

3.3 Hasil Uji Korelasi Pearson

Hasil uji korelasi Pearson menunjukkan adanya hubungan kuat antara variabel literasi digital dan kesiapan keamanan siber. Nilai koefisien korelasi (r) sebesar 0,67 dengan nilai $p < 0{,}01$ mengindikasikan bahwa semakin tinggi literasi digital, maka semakin tinggi pula kesiapan pelaku UMKM dalam menghadapi ancaman siber. Korelasi yang signifikan ini memperkuat pentingnya literasi digital sebagai faktor utama dalam ketahanan siber UMKM.

3.4 Hasil Uji Regresi Linier Sederhana

Dari hasil analisis regresi linier sederhana diperoleh model regresi:

$Y = a + bX + e$

Dengan hasil:

Koefisien b = 0,712

R^2 = 0,449

p-value < 0,01

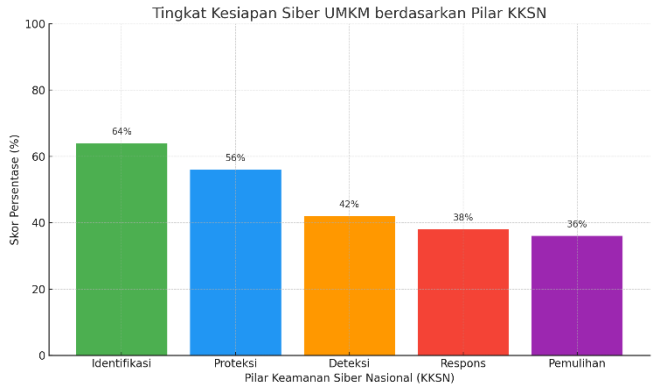
Interpretasi hasil ini menunjukkan bahwa literasi digital memiliki pengaruh yang signifikan terhadap kesiapan keamanan siber. Nilai R^2 sebesar 0,449 mengindikasikan bahwa 44,9% variasi kesiapan keamanan siber dapat dijelaskan oleh variabel literasi digital.

3.5 Hasil Konversi dan Visualisasi Pilar KKSN

Hasil konversi skor kesiapan keamanan siber berdasarkan lima pilar KKSN disajikan pada Tabel berikut:

Tabel 1. Tingkat Kesiapan Siber UMKM berdasarkan Pilar KKSN

Pilar KKSN	Skor Rata-rata	Skor Persentase	Kategori
Identifikasi	3.2	64%	Sedang
Proteksi	2.8	56%	Sedang
Deteksi	2.1	42%	Rendah
Respons	1.9	38%	Rendah
Pemulihan	1.8	36%	Rendah



Grafik 1. Visualisasi Tingkat Kesiapan Siber UMKM berdasarkan Pilar KKSN

Grafik di atas menunjukkan bahwa pilar "Identifikasi" memiliki skor tertinggi, sementara "Pemulihan" mencatatkan skor terendah. Skor yang tergolong "Rendah" pada sebagian besar pilar menunjukkan kurangnya kesiapan siber secara menyeluruh.

3.6 Pembahasan Temuan

Hasil penelitian menunjukkan bahwa meskipun pelaku UMKM telah memiliki kesadaran dalam mengidentifikasi aset digital, penerapan mekanisme deteksi, respons, dan pemulihan terhadap insiden siber masih sangat rendah. Ketimpangan ini menandakan adanya gap dalam strategi keamanan digital yang digunakan. Keterbatasan pemahaman teknis, minimnya pelatihan, serta tidak adanya kebijakan internal terkait keamanan siber menjadi faktor utama yang menyebabkan rendahnya skor pada tiga pilar tersebut.

Secara statistik, hubungan yang kuat antara literasi digital dan kesiapan siber menunjukkan bahwa peningkatan pemahaman dan kemampuan digital pelaku UMKM harus menjadi fokus utama dalam upaya mitigasi risiko. Literasi digital tidak hanya terkait dengan penggunaan teknologi, tetapi juga mencakup pemahaman tentang risiko, pengelolaan data, dan pengambilan keputusan dalam konteks keamanan informasi.

Temuan ini juga konsisten dengan hasil penelitian sebelumnya (Rombaldo et al., 2023; BSSN, 2022) yang menyatakan bahwa rendahnya literasi digital menjadi hambatan utama dalam implementasi keamanan siber di sektor UMKM. Oleh karena itu, diperlukan pendekatan kolaboratif antara pemerintah, sektor swasta, dan komunitas digital untuk memperkuat sistem pendukung keamanan siber, termasuk penyusunan SOP, pelatihan rutin, dan integrasi standar nasional keamanan informasi berbasis KKSN.

KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa tingkat kesiapan keamanan siber UMKM di Kota Balikpapan masih berada pada kategori rendah hingga sedang. Pilar identifikasi menunjukkan tingkat kesiapan tertinggi, yang mencerminkan adanya kesadaran awal terhadap pentingnya aset digital. Namun, pada aspek deteksi, respons, dan pemulihan, skor kesiapan masih tergolong rendah, menandakan lemahnya sistem dan prosedur yang diterapkan oleh UMKM dalam menghadapi ancaman siber. Analisis statistik menunjukkan bahwa terdapat hubungan yang kuat dan signifikan antara literasi digital dan kesiapan keamanan siber, dengan nilai korelasi (r) sebesar 0,67 dan koefisien determinasi (R^2) sebesar 0,449. Hal ini membuktikan bahwa peningkatan literasi digital memiliki pengaruh besar terhadap kesiapan UMKM dalam mengelola risiko keamanan digital. Temuan ini menegaskan bahwa literasi digital tidak hanya berkaitan dengan pemahaman teknologi, tetapi juga menyangkut kemampuan pelaku UMKM dalam melindungi data, mendeteksi anomali, serta merespons insiden siber secara tepat. Oleh karena itu, strategi mitigasi yang dirancang harus berfokus pada peningkatan kapasitas pelaku UMKM melalui pelatihan, penyusunan kebijakan

keamanan internal, serta dukungan berkelanjutan dari pihak pemerintah dan swasta dalam mendorong penerapan kerangka kerja keamanan siber nasional (KKSN) secara komprehensif dan aplikatif.

DAFTAR PUSTAKA

[1] Anan, M., Rahmah, S. A., & Risuhendri, R. (2024). *Meningkatkan Kesadaran Digital dalam Pencegahan Penipuan Online untuk Kelompok UMKM Desa Tanjung Haratan*. ABDI DALEM: Jurnal Pengabdian kepada Masyarakat, 1(2), 1–15. https://doi.org/10.70585/abdidalem.v1i2.29

[2] Anggita, W., Noviayanti Manik, J. D., & Zaliman, I. (2024). *Mitigasi Ancaman Social Engineering bagi UMKM melalui Program Sosialisasi di Kota Pangkalpinang*. Jurnal Abdimas Ilmiah Citra Bakti, 6(1), 1–10. https://doi.org/10.38048/jailcb.v6i1.4556

[3] Arikunto, S. (2019). *Prosedur Penelitian: Suatu Pendekatan Praktik*. Rineka Cipta.

Balafif, S. (2024). *Penyesuaian Model Ketahanan Siber UMKM di Indonesia dengan NIST Cybersecurity Framework*. Jurnal Informatika: Jurnal Pengembangan IT. https://ejournal.poltekharber.ac.id/index.php/informatika/article/view/5662

[4] Dananjoyo, S. W. (2024). *Literasi Digital di Kalangan Masyarakat Pedesaan: Upaya Meningkatkan Kesadaran Keamanan Siber*. Jurnal Edutein, 2(1), 1–15. https://www.ejurnal.unisri.ac.id/index.php/edute/article/view/11868

[5] Riandi, M. H., Putri, I. L. A., Rahman, H. A., & Kusumadewi, A. W. (2023). *Perilaku Keamanan Siber bagi UMKM*. Jurnal Pengabdian kepada Masyarakat Nusantara. https://ejournal.sisfokomtek.org/index.php/jpkm/article/view/2462

[6] Yulistyawati Evelina, T., Sulasari, A., Permatasari, I. R., Budiarti, L., & Sakti, R. J. N. (2024). *Literasi Digital untuk Peningkatan Kapasitas Pelaku Usaha Skala Mikro, Kecil dan Menengah di Kota Malang*. Jurnal Abdimas Polinema, 9(2). https://jurnal.polinema.ac.id/index.php/abdimas/article/view/2449

[7] Suartana, I. M., Putra, R. E., Bisma, R., & Prapanca, A. (2023). *Pengenalan Pentingnya Cyber Security Awareness pada UMKM*. Jurnal Abadimas Adi Buana. https://jurnal.unipasby.ac.id/index.php/abadimas/article/view/4560

[8] Shapiro, S. S., & Wilk, M. B. (1965). *An analysis of variance test for normality*. Biometrika, 52(3–4), 591–611. https://doi.org/10.1093/biomet/52.3-4.591