

## URGENSI MANAJEMEN KEAMANAN DAN PENGENDALIAN SISTEM INFORMASI BAGI UMKM DI INDONESIA

Mahendra Adhi Nugroho<sup>1</sup>, Agatha Yerika Septininditya<sup>2</sup>, R. Andro Ziliyo Nugraha<sup>3</sup>

<sup>1, 2, 3</sup>Universitas Negeri Yogyakarta, Jl. Colombo No.1, Sleman, Yogyakarta, Indonesia

Email: [mahendra@uny.ac.id](mailto:mahendra@uny.ac.id)

---

### Article History

Received: 22-06-2024

Revision: 29-06-2024

Accepted: 02-07-2024

Published: 03-07-2024

**Abstract.** In today's digital era, Micro, Small, and Medium Enterprises (MSMEs) are one of the important components in the national and global economy. In the context of MSMEs in Indonesia, managing and controlling information system security is a very important thing to pay attention to. This article discusses the urgency of steps that need to be taken to support the growth of MSMEs in Indonesia. The method used in this research is descriptive qualitative method. The approach used is library research. Based on the results of the literature study, it was found that the management and control of information systems really need to be applied to MSMEs in Indonesia. This is because threats to information systems and technology in MSMEs are unavoidable conditions. Generally, MSMEs already know this, but they have only taken the most basic information system management and control actions, and there are still many MSMEs that have not taken information system management and control actions.

**Keywords:** MSMEs, Management, Control, Information System Security

**Abstrak.** Di era digital saat ini, Usaha Mikro, Kecil, dan Menengah (UMKM) merupakan salah satu komponen penting dalam perekonomian nasional dan global. Dalam konteks UMKM di Indonesia, mengelola dan mengendalikan keamanan sistem informasi merupakan hal yang sangat penting untuk diperhatikan. Artikel ini membahas urgensi langkah-langkah yang perlu dilakukan untuk mendukung pertumbuhan UMKM di Indonesia. Metode yang digunakan dalam penelitian ini adalah metode kualitatif deskriptif. Pendekatan yang digunakan adalah studi kepustakaan (*library research*). Berdasarkan hasil studi literatur ditemukan bahwa pengelolaan dan pengendalian sistem informasi sangat perlu diterapkan pada UMKM di Indonesia. Hal ini dikarenakan ancaman terhadap sistem informasi dan teknologi pada UMKM merupakan kondisi yang tidak dapat dihindari. Umumnya UMKM sudah mengetahui hal ini, namun baru melakukan tindakan pengelolaan dan pengendalian sistem informasi yang paling dasar saja, dan masih banyak UMKM yang belum melakukan tindakan pengelolaan dan pengendalian sistem informasi.

**Kata Kunci:** UMKM, Manajemen, Kontrol, Keamanan Sistem Informasi

---

**How to Cite:** Nugroho, M. A., Septininditya, A. Y., & Nugraha, R. A. Z. (2024). Urgensi Manajemen Keamanan dan Pengendalian Sistem Informasi bagi UMKM di Indonesia. *Indo-Fintech Intellectuals: Journal of Economics and Business*, 4 (3), 734-744. <http://doi.org/10.54373/ifjeb.v4i3.1373>

---

### PENDAHULUAN

Indonesia merupakan negara yang memiliki jumlah Usaha Mikro, Kecil, dan Menengah (UMKM) terbanyak di ASEAN. Berdasarkan data dari ASEAN Investment Report 2022, pada tahun 2021 Indonesia akan memiliki jumlah UMKM terbanyak dengan 65,46 juta unit atau sekitar 90% dari jumlah UMKM di ASEAN (Isnani, 2022). Besarnya jumlah UMKM ini

dikarenakan mayoritas UMKM di Indonesia merupakan kegiatan usaha rumah tangga yang didominasi oleh usaha mikro. Sesuai Undang-Undang Nomor 20 Tahun 2008, Usaha mikro adalah usaha yang memiliki kekayaan bersih kurang dari Rp50.000.000,00.

Di era digital saat ini, Usaha Mikro, Kecil, dan Menengah (UMKM) merupakan salah satu komponen penting dalam perekonomian nasional dan global. Di Indonesia, UMKM memiliki kontribusi yang cukup besar terhadap Pendapatan Domestik Bruto (PDB), yaitu sebesar 60,5% atau sekitar Rp8.573 triliun setiap tahunnya. Selain itu, dalam kaitannya dengan penyerapan tenaga kerja, UMKM juga memiliki kontribusi yang cukup besar, yaitu sekitar 116 juta orang atau 97% dari total penyerapan tenaga kerja nasional (Kamar Dagang dan Industri (Kadin Indonesia, 2023). Berdasarkan kedua hal tersebut, dapat dikatakan bahwa UMKM merupakan tulang punggung perekonomian Indonesia. Untuk itu, UMKM harus terus mengembangkan diri agar perekonomian di Indonesia tetap stabil. Salah satu langkah yang dapat dilakukan UMKM untuk terus berkembang adalah dengan terbuka terhadap hal-hal baru. Apalagi saat ini kita sudah memasuki era digital dimana perlahan segala bentuk kegiatan mulai menjadi lebih mudah dengan adanya sistem informasi dan teknologi.

Sistem informasi dan teknologi telah banyak membantu Usaha Mikro, Kecil, dan Menengah (UMKM). UMKM dapat memanfaatkan teknologi untuk meningkatkan efisiensi kegiatan operasional, meningkatkan produktivitas, dan mempertahankan keunggulan kompetitif (Khan et al., 2020). Selain itu, keberadaan sistem informasi akuntansi juga memberikan pengaruh yang signifikan terhadap keberhasilan usaha kecil dan menengah (Lazuardi & Salam, 2019). Sehingga keberadaan sistem informasi dapat memberikan dampak terhadap pertumbuhan dan keberhasilan Usaha Mikro Kecil dan Menengah (UMKM). Namun, meskipun penggunaan sistem informasi sangat membantu kinerja UMKM, di sisi lain UMKM juga dihadapkan pada berbagai tantangan dalam menjalankan bisnisnya, terutama yang berkaitan dengan pengelolaan dan keamanan sistem informasi. Selain itu, UMKM sering kali kekurangan sumber daya dan keahlian untuk menerapkan dan memelihara langkah-langkah keamanan informasi yang kuat dengan benar, sehingga rentan terhadap berbagai ancaman (Marican *et al.*, 2023). Data menunjukkan bahwa selama Januari hingga Mei 2023 terdapat 764.015 deteksi file berbahaya yang menargetkan UMKM, eksploitasi merupakan ancaman paling umum bagi UMKM, terhitung 63 persen (483.980) dari seluruh deteksi selama lima bulan pertama tahun 2023 (Rochman, 2023).

Semakin banyaknya data bisnis yang bersifat rahasia, informasi pelanggan, dan aset penting lainnya yang disimpan dan ditransmisikan secara elektronik, maka kesadaran akan kontrol keamanan informasi yang komprehensif di sektor UMKM menjadi sangat penting.

Penelitian sebelumnya menyoroti risiko signifikan yang dihadapi UMKM di bidang ini (Khan et al., 2020). Selain itu, pembahasan yang dilakukan oleh peneliti sebelumnya terkait keamanan aset informasi pada UMKM yang telah menerapkan sistem TI juga masih sangat terbatas (Nugraha *et al.*, 2022). Usaha kecil sering menjadi target kejahatan siber karena postur keamanan yang umumnya lebih lemah dan kurangnya kesadaran manajemen (Rochman, 2023). Selain itu, gangguan pada sistem informasi di lingkungan UMKM dapat menimbulkan konsekuensi yang luas, berdampak pada stabilitas ekonomi nasional, kepercayaan publik, dan kelangsungan bisnis.

Urgensi penerapan kontrol dan keamanan sistem informasi pada UMKM tidak dapat diabaikan begitu saja. Dengan semakin banyaknya pelaku bisnis yang beralih ke model bisnis online, maka kebutuhan akan pengendalian dan keamanan sistem informasi semakin mendesak. Dalam konteks ini, UMKM perlu menyadari bahwa setiap aktivitas bisnis yang melibatkan sistem informasi harus dilakukan dengan pengendalian dan pengamanan yang tepat. Penelitian ini bertujuan untuk mengeksplorasi urgensi dan pentingnya pengelolaan dan pengendalian sistem informasi serta langkah-langkah keamanan yang kuat pada UMKM untuk menjaga sistem operasi mereka, melindungi data sensitif, dan memastikan kelangsungan bisnis.

## **METODE**

Metode yang digunakan dalam penelitian ini adalah metode kualitatif deskriptif. Pendekatan yang digunakan adalah studi kepustakaan (*library research*). Studi literatur dilakukan dengan cara mengkaji literatur dan referensi terkait yang relevan dengan objek penelitian ini. Objek penelitian yang dimaksud adalah artikel jurnal yang berkaitan dengan implementasi dan keamanan sistem informasi pada UMKM. Dengan menggunakan metode ini, peneliti akan mendapatkan pemahaman yang mendalam dan komprehensif mengenai pentingnya pengelolaan dan pengamanan sistem informasi bagi UMKM di Indonesia. Sehingga diharapkan penelitian ini dapat memberikan kontribusi baik secara praktis maupun teoritis bagi UMKM dan pihak-pihak terkait lainnya. Pengumpulan data dilakukan melalui artikel ilmiah yang dipublikasi pada berbagai jurnal dan terindeks pada basis data *google scholar*. Analisis data dilakukan secara kualitatif yang terdiri dari reduksi data, penyajian data, dan penarikan kesimpulan.

## HASIL

UMKM (Usaha Kecil, Mikro, dan Menengah) sangat erat kaitannya dengan sistem informasi dan teknologi (Farhani & Chaniago, 2021). Sistem informasi merupakan bagian integral dari operasi UMKM, membantu mereka mengelola, mengumpulkan, dan menginterpretasikan data yang diperlukan untuk pengambilan keputusan bisnis. Dengan demikian, melalui sistem informasi, UMKM dapat meningkatkan efisiensi, daya saing, dan kualitas layanan yang diberikan kepada pelanggan (Basry & Sari, 2018). Selain itu, berdasarkan hasil penelitian, sistem informasi akuntansi terbukti memiliki pengaruh positif terhadap kinerja UMKM (Prasetyo & Ambarwati, 2021). Hal ini berarti semakin baik penggunaan sistem informasi akuntansi pada UMKM, maka akan semakin baik pula kinerja UMKM tersebut.

Penggunaan sistem informasi untuk UMKM dapat dilakukan untuk mengelola data-data yang dibutuhkan untuk mengambil keputusan bisnis. Data tersebut dapat berupa informasi pelanggan, data transaksi, dan produk yang dijual. Data tersebut kemudian diolah melalui sistem informasi dan diperoleh hasil yang dapat meningkatkan efisiensi operasional dengan melakukan otomatisasi proses bisnis. Kegiatan yang dapat dilakukan oleh sistem informasi antara lain pengelolaan inventori, pengelolaan data pengiriman dan pengelolaan data penjualan, menghasilkan data sebagai bahan penyusunan strategi untuk meningkatkan daya saing, menghasilkan data yang dapat memberikan informasi yang akurat dan cepat mengenai pasar, kompetitor, dan pelanggan, serta meningkatkan kualitas pelayanan dengan memberikan informasi yang akurat dan cepat mengenai kebutuhan pelanggan. Sehingga UMKM dapat memberikan pelayanan yang lebih baik dan membantu UMKM dalam meningkatkan pengelolaan keuangan dengan memberikan informasi yang akurat dan cepat mengenai pendapatan, biaya dan kinerja keuangan.

UMKM juga tidak bisa lepas dari teknologi digital. Teknologi digital telah membuka pintu akses UMKM ke pangsa pasar global melalui platform *e-commerce* seperti Tokopedia, Bukalapak, dan Shopee. Sehingga UMKM dapat memperluas jangkauan produknya hingga ke luar negeri, meningkatkan omzet dan mencapai pertumbuhan yang lebih luas. Selain itu, teknologi digital juga memberikan peluang bagi UMKM untuk mendapatkan informasi pasar melalui *platform* media sosial seperti *Facebook*, *Instagram*, dan *Twitter*. Dengan data mengenai kebutuhan pelanggan dan tren pasar, UMKM dapat merancang strategi pemasaran yang lebih cerdas dan mengembangkan produk yang sesuai dengan kebutuhan pasar.

Keberadaan sistem informasi mampu memberikan kemudahan dan meningkatkan efisiensi serta keuntungan UMKM. Namun, keberadaan sistem informasi ini juga memberikan tantangan tersendiri bagi UMKM. Apalagi saat ini orang yang ingin melakukan penipuan, peretasan, atau sabotase secara online dapat melakukannya dengan mudah, hanya dengan mengikuti langkah-langkah dan menonton video tutorial yang ada di internet. Sehingga penting bagi UMKM untuk dapat mengelola dan mengendalikan sistem informasi sebagai bentuk antisipasi, pencegahan atau upaya untuk mengurangi tingkat resiko jika terjadi penipuan atau serangan komputer. Untuk mengetahui urgensi pengelolaan dan pengendalian sistem informasi pada UMKM, peneliti melakukan studi literasi terhadap delapan artikel jurnal. Delapan artikel jurnal tersebut memiliki tema yang berkaitan dengan keamanan sistem informasi dan implementasinya pada UMKM. Hasil studi literasi diuraikan pada Tabel 1.

**Tabel 1.** Hasil studi literasi

No.	Nama Penulis/Tahun	Judul	Hasil penelitian
1	(Nugraha <i>et al.</i> , 2022)	Studi Literatur: Analisis Implementasi Keamanan Aset Informasi Dalam Mendukung Pengembangan UMKM di Indonesia	Hanya ada beberapa UMKM yang sudah menerapkan sistem keamanan aset informasi dalam kegiatan operasionalnya, namun sistem keamanan aset informasi tersebut masih sangat terbatas.
2	(Álvarez <i>et al.</i> , 2022)	Model untuk Mengukur Risiko Keamanan Siber pada UMKM di Tecomán, Colima	Risiko keamanan siber yang harus dicegah oleh UMKM adalah manipulasi atau pembocoran file dan data baik perusahaan maupun pengguna oleh orang dalam atau luar perusahaan, kerusakan peralatan atau server, sumber daya manusia yang tidak memiliki pemahaman tentang masalah keamanan, adanya software berbahaya atau infeksi virus komputer, tidak adanya aturan atau kebijakan penggunaan komputer, email, jaringan, internet, dan perangkat lain di perusahaan
3	(Díaz-Piraquive, Muriel-Perea and González-Crespo, 2023)	Manajemen Keamanan Siber adalah Usaha Mikro, Kecil, dan Menengah di Columbia	Beberapa perusahaan sudah mengetahui tentang ancaman pada sistem informasi, namun meskipun perusahaan mengetahui apa saja ancaman pada sistem informasi dan keamanan siber, mereka tidak melakukan mitigasi risiko terhadap ancaman serangan siber.
4	(Thamrongthanakit, 2023)	Dampak Praktik Keamanan Siber terhadap Kerusakan dan Perlindungan Serangan Siber di Kalangan Usaha Kecil dan Menengah di Thailand	Menerapkan keamanan dan kontrol dunia maya di UKM penuh dengan kesulitan, yang paling utama adalah kekurangan dana, personel, dan keahlian. Oleh karena itu, bagi UKM, keamanan siber tidak dianggap sepenting tujuan perusahaan lainnya.

No.	Nama Penulis/Tahun	Judul	Hasil penelitian
5	(Zamsuri, Syafitri and Syahputra Pane, 2021)	Evaluasi Kesadaran Keamanan Informasi pada Pemasaran Digital (Studi Kasus UMKM di Indonesia)	Di era teknologi informasi saat ini, pengetahuan tentang keamanan informasi sangatlah penting. Setiap karyawan harus memiliki pengetahuan tentang keamanan informasi. Rahasia untuk menghentikan munculnya ancaman keamanan informasi adalah kewaspadaan.
6.	(Abdurohim, 2023)	Analisis Tantangan dan Peluang UMKM di Era Digital	UMKM harus lebih sadar akan masalah keamanan siber. UKMM harus berinvestasi dalam sistem keamanan, membuat kebijakan privasi data, dan menawarkan sumber daya bantuan teknis untuk perlindungan data. Karena ini semua adalah tindakan penting untuk melindungi data,
7.	(Ikuro and Zeng, 2022)	Meningkatkan pelaporan insiden keamanan siber di Nigeria: perspektif usaha mikro dan kecil	Pemerintah Nigeria telah memberikan perhatian khusus terhadap ancaman sistem informasi dan mitigasi keamanan siber pada UKM. Hal ini tertuang dalam sebuah saluran khusus yang menampung laporan dari masyarakat jika terjadi serangan terhadap sistem informasi. Namun, ternyata masih banyak UKM yang belum mengetahui saluran dan organisasi untuk melaporkan insiden keamanan siber.
8	(Pawar and Palivela, 2022)	LCCI: Kerangka kerja untuk kontrol keamanan siber yang paling sedikit diterapkan untuk usaha kecil dan menengah (UKM)	Masalah utama yang diidentifikasi selama penelitian termasuk kurangnya dana untuk membangun keamanan sistem informasi, UMKM tidak dapat menemukan kontrol keamanan siber yang cocok untuk mereka, kurangnya sumber daya yang terampil, dan UMKM tidak dapat menjadikan penerapan keamanan siber sebagai prioritas bisnis.

## DISKUSI

Pada Tabel 1, ditampilkan hasil penelitian terdahulu mengenai penerapan keamanan siber di UMKM. Penelitian dilakukan di berbagai lokus, tidak hanya di Indonesia tetapi dari negara lain seperti Thailand, Nigeria, Kolombia dan Meksiko. Penelitian pertama mendapatkan hasil bahwa tidak semua UMKM menerapkan keamanan pada sistem informasi. Beberapa UMKM memang terlihat memiliki kesadaran akan pentingnya pengamanan sistem informasi, namun masih ada UMKM yang belum menerapkan keamanan pada sistem informasi (Nugraha *et al.*, 2022). Setiap UMKM yang telah menerapkan sistem keamanan melakukannya dengan tingkat keamanan yang berbeda-beda. Namun, sebagian besar melakukan keamanan tingkat dasar,

misalnya pengaturan password pada komputer, *handphone*, dll. Sehingga temuan dari penelitian ini menunjukkan bahwa pembahasan mengenai penerapan Sistem Informasi di UMKM masih jauh dari yang diharapkan. Hal ini dikarenakan UMKM merupakan badan usaha yang memiliki risiko yang sama dengan badan usaha lainnya, seperti pencurian data, modifikasi informasi, dan penggunaan data informasi secara ilegal, namun pengamanan yang dilakukan oleh UMKM masih sangat minim dan belum sepadan dengan ancaman yang dihadapinya.

Pada penelitian kedua, peneliti mendapatkan hasil bahwa terdapat beberapa risiko keamanan siber yang harus dicegah oleh UMKM. Risiko manipulasi atau kebocoran file dan data baik perusahaan maupun pengguna oleh orang di dalam atau di luar perusahaan, kerusakan peralatan atau server, kurangnya kesadaran dan pelatihan staf tentang masalah keamanan, penerapan perangkat lunak berbahaya atau terinfeksi virus, kurangnya peraturan atau kebijakan terkait penggunaan komputer, email, jaringan, internet, dan peralatan teknologi lainnya di perusahaan (Álvarez *et al.*, 2022). Dari hasil yang diperoleh dari instrumen pengumpulan data, beberapa poin yang menonjol menurut tanggapan UMKM adalah beberapa UMKM yang persentase penggunaan sistem informasinya cukup besar lebih waspada terhadap keamanan siber. Namun, di satu sisi, sebagian besar dari mereka masih belum memiliki atau tidak mengetahui apakah ada rencana darurat yang mungkin timbul akibat masalah teknologi.

Penelitian ketiga melakukan analisis terhadap manajemen keamanan siber pada usaha mikro, kecil, dan menengah di Kolombia. Hasil dari penelitian tersebut menunjukkan bahwa sebagian besar UMKM di Kolombia mengetahui apa itu keamanan siber dan prosedur utama yang mereka jalankan. Namun meskipun perusahaan mengetahui apa itu keamanan siber, mereka tidak mengembangkan langkah-langkah untuk mengurangi risiko yang berasal dari ancaman serangan siber (Piraquive *et al.*, 2023). Hal ini dikarenakan sebagian besar UMKM tidak memiliki pedoman untuk menentukan unit mana di dalam UMKM yang bertanggung jawab dalam mengelola keamanan siber, dan perjanjian kerahasiaan data dengan pihak ketiga masih sulit untuk diimplementasikan. Sehingga disimpulkan bahwa pedoman tersebut terkait dengan langkah-langkah untuk mengelola dan mengamankan sistem informasi penting bagi UMKM.

Temuan dari penelitian keempat menunjukkan bahwa ransomware, malware, dan serangan web merupakan serangan siber yang paling sering dialami oleh UKM. Banyak peserta penelitian yang berpikir bahwa karena gangguan semacam ini sangat sering terjadi, mereka dapat menanganinya tanpa menerapkan strategi keamanan siber. Gagasan bahwa UKM tidak memerlukan tindakan pencegahan keamanan siber yang ketat karena mereka memiliki proses

bisnis dan teknologi yang sederhana mendukung kesimpulan ini. Menurut sudut pandang yang berbeda, UKM tidak perlu menggunakan kerangka kerja keamanan siber karena implementasinya yang rumit dan kebutuhan sumber daya yang tinggi. Meskipun sebagian besar UKM dalam penelitian ini memiliki sistem yang tidak terlalu rumit, mereka masih hanya membutuhkan beberapa kontrol keamanan siber untuk melindungi dari serangan siber tertentu yang dapat membahayakan perusahaan mereka. Salah satu kontrol tersebut adalah penggunaan firewall aplikasi web untuk memfilter, memantau, dan menghentikan lalu lintas malware berbahaya serta serangan DDoS. Satu-satunya pengecualian adalah beberapa UKM di sektor perbankan dan TI yang telah menerapkan kerangka kerja keamanan siber. Namun, pendorong utama adopsi kerangka kerja keamanan siber yang disebutkan oleh UKM dalam penelitian ini tidak terkait dengan keamanan, tetapi lebih terkait dengan tuntutan pelanggan, penegakan hukum, dan kepercayaan diri mereka sendiri. Karena persepsi mereka bahwa layanan terkelola mematuhi peraturan dan standar keamanan siber, mayoritas UKM dalam penelitian kami bergantung pada layanan tersebut. Hasilnya, mereka dapat melanjutkan tanpa harus menyiapkan arsitektur keamanan siber mereka sendiri di dalam perusahaan mereka

Studi kelima, yang menilai UMKM di Indonesia, terkendala oleh sedikitnya jumlah UMKM yang berpartisipasi. Hanya 17 dari 384 UMKM yang diminta yang berhasil dikumpulkan. Uji reliabilitas, validitas, dan normalitas yang dihasilkan dari pengolahan data dengan data ini cukup baik. Temuan penelitian ini menunjukkan bahwa, di era teknologi informasi saat ini, pengetahuan tentang keamanan informasi sangat penting. Setiap karyawan harus memiliki pengetahuan tentang keamanan informasi. Pertahanan terbaik terhadap munculnya ancaman keamanan informasi adalah kewaspadaan. Namun, tidak semua UMKM memiliki pengetahuan tentang kontrol dan manajemen sistem informasi.

Menurut studi keenam, Usaha Mikro, Kecil, dan Menengah (UMKM) menghadapi berbagai masalah di era digital yang membutuhkan solusi komprehensif. Akses dan pemahaman terhadap teknologi merupakan penghalang utama, terutama dalam hal penggunaan uang digital. Kurangnya pengetahuan tentang teknologi dan literasi digital merupakan penghalang terbesar bagi pemilik UMKM. Program pelatihan dan pendanaan dari pemerintah dan lembaga pendidikan diperlukan untuk mengatasi hal ini. Masalah lainnya adalah keamanan digital, di mana UMKM perlu lebih sadar akan keamanan siber. Tindakan penting yang perlu dilakukan adalah menerapkan kebijakan privasi data, mengedukasi masyarakat tentang perlindungan data, dan membeli peralatan keamanan. UMKM dipaksa oleh persaingan lokal dan internasional yang semakin ketat untuk berinovasi, menggunakan teknik pemasaran digital, dan berpartisipasi.

Penelitian ketujuh membahas pelaporan insiden keamanan siber di UMK Nigeria. Penelitian ini lebih lanjut menekankan langkah-langkah yang telah diambil pemerintah Nigeria untuk memastikan keamanan siber dan ketahanan UMK terhadap serangan siber. Untuk itu, pemerintah berpartisipasi dengan membuat kebijakan dan mitigasi keamanan siber. Hal ini tertuang dalam kanal khusus yang menampung laporan dari masyarakat jika terjadi serangan terhadap sistem informasi. Namun, ternyata masih banyak pelaku UKM yang belum mengetahui kanal dan organisasi untuk melaporkan insiden keamanan siber. Hasil dari penelitian terbaru adalah perlu adanya implementasi *cyber security*, walaupun implementasi ini masih minim dan bertahap, hal ini akan berguna bagi UKM untuk mengatasi resiko peretasan.

Hasil studi literatur menyatakan bahwa penting untuk mengelola dan mengendalikan sistem informasi untuk UMKM. Meskipun ada pandangan bahwa serangan siber merupakan hal yang biasa terjadi, namun kerangka kerja keamanan siber tidak diperlukan dan diyakini bahwa UMKM memiliki proses dan sistem bisnis yang sederhana, sehingga tidak memerlukan tindakan keamanan siber yang ketat. Namun, fakta mengenai kerugian yang diakibatkan oleh serangan siber tidak dapat dipungkiri. Memiliki manajemen dan kontrol sistem informasi dapat meminimalisir risiko yang mungkin diterima oleh UMKM jika terjadi serangan siber

## **KESIMPULAN**

Berdasarkan hasil studi literatur terhadap delapan jurnal, ditemukan bahwa pengelolaan dan pengendalian sistem informasi sangat perlu diterapkan pada UMKM di Indonesia. Hal ini dikarenakan ancaman terhadap sistem informasi dan teknologi pada UMKM merupakan kondisi yang tidak dapat dihindari. Umumnya UMKM sudah mengetahui hal ini, namun baru melakukan tindakan pengelolaan dan pengendalian sistem informasi yang paling dasar saja, dan masih banyak UMKM yang belum melakukan tindakan pengelolaan dan pengendalian sistem informasi. Alasan dari hal tersebut adalah beberapa UMKM belum memiliki pengetahuan tentang dampak krusial dari kecurangan komputer, manajemen memiliki pandangan bahwa UMKM merupakan unit kecil sehingga tidak perlu adanya pengamanan khusus untuk sistem informasi yang mereka miliki, beberapa UMKM memiliki pandangan bahwa sistem informasi sangat dibutuhkan namun mereka belum memiliki panduan untuk menerapkan pengelolaan dan pengendalian sistem informasi tersebut sehingga cenderung tidak mengetahui langkah apa yang harus mereka lakukan. Pada kedelapan jurnal di atas, Nigeria menjadi satu-satunya negara yang telah menyediakan fasilitas bagi UMKM berupa kanal khusus yang menampung laporan dari masyarakat jika terjadi serangan terhadap sistem

informasi. Di Indonesia, tingkat penipuan dengan menggunakan media komputer cukup tinggi, sehingga apa yang dilakukan oleh pemerintah Nigeria ini juga bisa dimodifikasi dan diterapkan di Indonesia.

## REFERENSI

- Abdurohim, D. (2023) 'Analysis of MSME Challenges and Opportunities In The Digital Era', *International Journal of Economic Literature*, 9(3), pp. 356–363.
- Adi Saputra, L. et al. (2023) 'Ancaman Keamanan Pada Sistem Informasi Manajemen Perusahaan', *Jurnal Pendidikan Siber Nusantara*, 1(2), pp. 58–66. Available at: <https://doi.org/10.38035/jpsn.v1i2.48>.
- Álvarez, F.P. et al. (2022) 'Model for Measuring Cybersecurity Risks in MSMEs in Tecomán, Colima', *Asociacion Nacional de Instituciones de Education en Tecnologias de la Informacion*, pp. 1–83.
- Basry, A. and Sari, E.M. (2018) 'Penggunaan Teknologi Informasi dan Komunikasi (TIK) pada Usaha Mikro, Kecil dan Menengah (UMKM)', *IKRA-ITH INFORMATIKA: Jurnal Komputer dan Informatika*, 2(3), pp. 53–60. Available at: <http://journals.upi-yai.ac.id/index.php/ikraith-informatika/article/view/266>.
- Díaz-Piraquive, F.N., Muriel-Perea, Y. de J. and González-Crespo, R. (2023) *Cybersecurity Management in Micro, Small, and Medium Enterprises in Colombia*. Edited by L. Uden and I.-H. Ting. Springer Science and Business Media Deutschland GmbH. Available at: <https://pure.urosario.edu.co/en/publications/cybersecurity-management-in-micro-small-and-medium-enterprises-in>.
- Farhani, I. and Chaniago, H. (2021) 'Faktor Penentu Transformasi Digital UMKM: Bukti dari Indonesia', *Prosiding The 12th Industrial Research Workshop and National Seminar*, pp. 1010–1015.
- Farina, K. and Opti, S. (2023) 'Pengaruh Pemanfaatan Sistem Informasi Akuntansi Dan Penggunaan Teknologi Informasi Terhadap Kinerja Umkm', *Jurnal Ekonomi & Ekonomi Syariah*, 6(1), pp. 704–713. Available at: <https://doi.org/10.36778/jesy.v6i1.1007>.
- Hanim, L. and Noorman, M. (2018) *UMKM (Usaha Mikro, Kecil, & Menengah) & Bentuk-Bentuk Usaha*. Edited by D.R. Hartono. UNISSULA PRESS.
- Ikuero, F.E. and Zeng, W. (2022) 'Improving cybersecurity incidents reporting in Nigeria: micro and small enterprises perspectives', *Nigerian Journal of Technology*, 41(3), pp. 512–520. Available at: <https://doi.org/10.4314/njt.v41i3.10>.
- Isnani, H. (2022) *5 Negara ASEAN dengan Jumlah UMKM Terbanyak, Nomor 2 Kontribusi ke Ekspor Tembus Rp1.267 Triliun*, *SindoNews.Com*. Available at: <https://ekbis.sindonews.com/read/951539/34/5-negara-asean-dengan-jumlah-umkm-terbanyak-nomor-2-kontribusi-ke-ekspor-tembus-rp1267-triliun-1669356702>.
- Jogiyanto, H.M. (2005) *Sistem teknologi informasi*. Yogyakarta: Andi.
- Kamar Dagang dan Industri (Kadin) Indonesia (2023) *UMKM Indonesia, Kadin Indonesia*. Available at: <https://kadin.id/data-dan-statistik/umkm-indonesia/>.
- Khan, M.I., Tanwar, S. and Rana, A. (2020) 'The need for information security management for SMEs', *Proceedings of the 2020 9th International Conference on System Modeling and Advancement in Research Trends, SMART 2020*, pp. 328–332. Available at: <https://doi.org/10.1109/SMART50582.2020.9337108>.
- Lazuardi, Y. and Salam, F.A. (2019) 'Pengaruh Penggunaan Sistem Informasi Akuntansi Terhadap Keberhasilan Usaha Kecil Menengah', *Jurnal Ilmiah Akuntansi Peradaban*, V(1), pp. 197–209.

- Marican, M.N.Y. *et al.* (2023) 'Cyber Security Maturity Assessment Framework for Technology Startups: A Systematic Literature Review', *IEEE Access*, 11, pp. 5442–5452. Available at: <https://doi.org/10.1109/ACCESS.2022.3229766>.
- Nugraha, I.S. *et al.* (2022) 'Studi Literatur: Analisis Implementasi Keamanan Aset Informasi Dalam Mendukung Pengembangan UMKM di Indonesia', *Jurnal Ekonomi dan Keuangan Syariah*, 01(02), pp. 253–262. Available at: <https://jurnal.perima.or.id/index.php/JEKSYa>.
- Pangesti, R.A.M., Anggraini, O. and Rachma, A.L.O. (2024) 'Penguatan UMKM melalui Digitalisasi dan Analisis SWOT Kampung Cyber Kelurahan Patehan Yogyakarta', *Managemen Business Innovation Conference-MBI*, 7, pp. 1006–1017. Available at: <https://jurnal.untan.ac.id/index.php/MBIC/index>.
- Pawar, S. and Palivela, D.H. (2022) 'LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs)', *International Journal of Information Management Data Insights*, 2(1), p. 100080. Available at: <https://doi.org/10.1016/j.jjime.2022.100080>.
- Prasetyo, A.S. and Ambarwati, L. (2021) 'Pengaruh Sistem Informasi Akuntansi Terhadap Kinerja UMKM Daerah Istimewa Yogyakarta', *Jurnal Riset Akuntansi dan Bisnis Indonesia*, 1(1), pp. 73–84. Available at: <https://doi.org/10.32477/jrabi.v1i1.xxx>.
- Rochman, F. (2023) *Laporan Kaspersky mengungkapkan bahwa UMKM masih menjadi sasaran penjahat dunia maya*, *Partaipandai.id 2023*. Available at: <https://partaipandai.id/laporan-kaspersky-mengungkapkan-bahwa-umkm-masih-menjadi-sasaran-penjahat-dunia-maya/>.
- Romney, M.B. *et al.* (2021) *Accounting Information Systems*. Harlow: Pearson Education Limited.
- Thamrongthanakit, T. (2023) *Impacts of Cybersecurity Practices on Cyberattack Damage and Protection Among Small and Medium Enterprises in Thailand*. Edited by M.S.A. El Mekawy. Stockholm University.
- UU No. 20 Tahun 2008 (2008) *Undang-Undang Republik Indonesia Nomor 20 Tahun 2008*. Indonesia.
- Wibowo, W.S., Yunanto and Prasetyo, M.H. (2020) 'Tinjauan Yuridis Terhadap Pemberian Kredit Kepada Usaha Mikro Kecil Dan Menengah (Umk) Oleh Bank Umum', *Notarius*, 13(2), pp. 710–726. Available at: <https://doi.org/10.14710/nts.v13i2.31096>.
- Yusnanto, T. *et al.* (2023) 'Pelatihan Dasar Keamanan Digital Untuk Mengurangi Pencurian Data Yang Berdampak Pada UMKM', *Jurnal Pengabdian Masyarakat Bangsa*, 1(9), pp. 2022–2029. Available at: <https://doi.org/10.59837/jpmba.v1i9.458>.
- Zamsuri, A., Syafitri, W. and Syahputra Pane, E. (2021) 'Evaluation of Information Security Awareness on Digital Marketing (Case Study of MSME in Indonesia)', 2(1), pp. 192–210. Available at: <https://doi.org/10.30880/ahcs.2021.02.01.020>.