P-ISSN: | E-ISSN:
Vol. 1, No. 1, Februari 2025, p. 1-6

Journal of SONIC

Research Article [OPEN ACCESS]

Framework Keamanan Siber (*Cybersecurity Hygiene*) Tingkat Dasar untuk Melindungi Data dan Transaksi Digital UMKM Menggunakan Pendekatan *Human-Centered Design*

Rima Aulia[1], Novi Hardiansyah[2]
Teknologi Rekayasa Perangkat Lunak, Politeknik Bisnis Digital Indonesia, Indonesia[1,2]

Email: rimaaulia@polbis.ac.id[1], nvhardiansyah@polbis.ac.id[2]

ABSTRAK

Transformasi digital UMKM meningkatkan kerentanan terhadap ancaman siber. Namun, solusi keamanan yang ada seringkali terlalu teknis dan tidak sesuai dengan kapasitas sumber daya serta literasi digital pelaku UMKM. Penelitian ini bertujuan mengembangkan sebuah *framework* keamanan siber tingkat dasar (*cybersecurity hygiene*) yang praktis, mudah diadopsi, dan berpusat pada manusia (*Human-Centered Design*/HCD) untuk melindungi data dan transaksi digital UMKM. Metode kualitatif dengan pendekatan HCD diterapkan melalui empat tahap: (1) *Empathize*, menggunakan wawancara mendalam (*in-depth interview*) dengan 15 pemilik UMKM dan FGD dengan 5 pakar keamanan siber untuk memahami perilaku, pengetahuan, dan hambatan; (2) *Define*, dengan membangun persona dan *user journey map* untuk mendefinisikan masalah inti; (3) *Ideate*, menghasilkan prototipe berupa *toolkit checklist* dan pedoman visual; (4) Test, melakukan *usability testing* terhadap prototipe dengan 10 partisipan UMKM. Analisis tematik (*thematic analysis*) pada data kualitatif mengungkap tiga tema utama: persepsi rendah terhadap risiko siber, kesenjangan besar antara pengetahuan dan praktik, serta kebutuhan akan panduan yang kontekstual dan non-teknis. *Framework* akhir yang dihasilkan, bernama "SIBER UMKM", terdiri dari tiga pilar (*Awareness, Basic-Hygiene, Incident Response*) dan diwujudkan dalam *dashboard* dan kartu pedoman visual. Hasil *usability testing* menunjukkan peningkatan pemahaman dan niat untuk menerapkan praktik keamanan sebesar 85%. Penelitian ini berkontribusi pada literasi keamanan siber inklusif dan mendukung pencapaian SDG 9 (Industri, Inovasi, dan Infrastruktur) dengan membangun ketahanan digital UMKM. *Framework* ini direkomendasikan untuk diadopsi oleh pendamping UMKM dan asosiasi sebagai materi pelatihan standar.

Kata Kunci: Keamanan Siber, *Cybersecurity Hygiene*, UMKM, *Human-Centered Design, Framework,* Analisis Tematik.

1. PENDAHULUAN

Usaha Mikro, Kecil, dan Menengah (UMKM) merupakan pilar fundamental perekonomian Indonesia, yang kini semakin gencar melakukan adopsi teknologi digital untuk meningkatkan daya saing dan pertumbuhan. Transisi ini, meski vital, membawa serta eksposur baru terhadap ancaman keamanan siber seperti *phishing, ransomware*, dan pencurian data. Risiko ini semakin mengkhawatirkan mengingat aset digital UMKM—mulai dari data pelanggan, catatan keuangan, hingga kredensial *platform e-commerce*—sering kali tidak dilindungi dengan memadai.

Ironisnya, meski kerentanan tinggi, perhatian terhadap keamanan siber di kalangan UMKM masih sangat minim. Studi sebelumnya (Alshaikh et al., 2022) menunjukkan bahwa pelaku UMKM seringkali menganggap diri mereka bukan target menarik bagi penyerang siber, sebuah persepsi yang keliru

mengingat nilai kumulatif data yang mereka miliki. Solusi keamanan yang tersedia di pasar juga mayoritas dirancang untuk korporasi besar, sehingga terlalu kompleks, mahal, dan teknis untuk konteks sumber daya dan literasi digital yang terbatas pada UMKM.

Kesenjangan ini menuntut pendekatan yang berpusat pada pengguna (*human-centric*), di mana solusi dirancang berdasarkan pemahaman mendalam tentang kebutuhan, perilaku, dan kendala nyata pelaku UMKM. Pendekatan *Human-Centered Design* (HCD) menawarkan metodologi yang tepat untuk merancang intervensi yang tidak hanya efektif secara teknis tetapi juga mudah diadopsi, praktis, dan sesuai dengan alur kerja bisnis sehari-hari. Penelitian ini berargumen bahwa peningkatan *cybersecurity hygiene*—praktik dasar kebersihan digital—merupakan langkah pertama yang paling krusial dan realistis.

Oleh karena itu, penelitian ini bertujuan untuk mengembangkan sebuah *framework* keamanan siber tingkat dasar dengan pendekatan HCD yang komprehensif. Fokusnya adalah menciptakan sebuah *toolkit* panduan dan alat yang dapat secara langsung melindungi data dan transaksi digital UMKM, sekaligus meningkatkan kesadaran dan kapasitas mereka. Penelitian ini berkontribusi pada pencapaian SDG 9, khususnya target 9.b yang mendukung pengembangan teknologi dan inovasi yang dapat diakses oleh semua pelaku usaha, termasuk UMKM.

2. METODE PENELITIAN

Penelitian ini menggunakan paradigma kualitatif dengan menerapkan metodologi *Human-Centered Design* (HCD) yang diadaptasi dari model *Double Diamond* (Design Council, 2019). HCD dipilih karena menempatkan pengguna (pelaku UMKM) sebagai inti dari setiap tahap perancangan solusi, sehingga memastikan hasil akhir yang relevan, dapat digunakan (*usable*), dan bernilai. Penelitian dilakukan dalam empat fase iteratif: *Discover & Empathize, Define, Develop,* dan *Deliver,* dengan partisipan utama adalah pelaku UMKM dari sektor kuliner dan retail yang telah aktif bertransaksi digital.

2.1. Fase 1: *Discover* and E*mpathize*

Fase ini bertujuan memahami konteks, motivasi, dan tantangan pengguna secara mendalam. Teknik pengumpulan data utama adalah wawancara mendalam (*in-depth interview*) semi-terstruktur terhadap 15 pemilik UMKM. Pertanyaan difokuskan pada pengalaman mereka dengan teknologi digital, kesadaran akan ancaman siber, praktik keamanan yang telah diterapkan, dan hambatan yang dirasakan. Selain itu, satu sesi *Focus Group Discussion* (FGD) diadakan dengan 5 orang pakar (2 akademisi informatika, 2 praktisi keamanan siber, 1 pendamping UMKM dari dinas setempat) untuk mendapatkan perspektif teknis dan kebijakan. Seluruh percakapan direkam dan ditranskrip secara verbatim. Analisis awal dilakukan dengan membuat *Empathy Map* untuk setiap profil UMKM, yang memetakan apa yang mereka pikirkan, rasakan, katakan, dan lakukan terkait keamanan digital.

2.2. Fase 2: Define

Pada fase ini, data dari Fase 1 dianalisis secara sistematis menggunakan *Thematic Analysis* (Braun & Clarke, 2006) untuk mengidentifikasi pola dan tema inti. Proses analisis meliputi: (1) *Familiarization* dengan membaca transkrip berulang kali; (2) *Generating initial codes* terhadap potongan data yang relevan; (3) *Searching for themes* dengan mengelompokkan kode yang serupa; (4) *Reviewing themes*; (5) *Defining and naming themes*; dan (6) *Producing the report.* Hasil analisis ini menghasilkan beberapa tema kunci seperti "Ilusi Keamanan" dan "Paradoks Kemudahan vs. Kerumitan". Tema-tema ini kemudian digunakan untuk membangun dua Persona utama (contoh: "Budi, pengusaha kuliner yang sibuk") dan dua User *Journey Map* yang memvisualisasikan titik-titik kritis (*pain points*) kerentanan siber dalam alur bisnis mereka, seperti saat mengunggah bukti transfer atau membagikan akses akun *marketplace* kepada karyawan.

2.3. Fase 3: *Develop* (*Ideate & Prototype*)

Berdasarkan pemahaman yang telah didefinisikan, tim peneliti melakukan sesi *ideation* untuk menghasilkan berbagai konsep solusi. Prinsip utamanya adalah kesederhanaan, visual, dan aksi segera (*actionable*). Konsep terpilih adalah sebuah framework "SIBER UMKM" yang terdiri dari tiga pilar. Konsep ini kemudian diwujudkan dalam dua bentuk prototipe *low-fidelity*: (1) Kartu Pedoman Visual (*Checklist*) berisi 10 langkah *hygiene* dasar dengan ikon dan bahasa yang sederhana; dan (2) Sketsa *Dashboard* Digital yang menyajikan status keamanan dalam bentuk lampu lalu lintas (hijau, kuning, merah). Sebuah *Basic Risk Assessment Matrix* sederhana juga dikembangkan untuk membantu UMKM mengidentifikasi dan memprioritaskan ancaman berdasarkan tingkat keparahan dan kemungkinan terjadinya.

2.4. Fase 4: *Deliver* (*Test & Refine*)

Prototipe diuji melalui *usability testing* dengan 10 partisipan UMKM baru yang memenuhi kriteria serupa. Partisipan diminta untuk menyelesaikan serangkaian tugas (*task scenario*), seperti "identifikasi dua risiko keamanan di toko *online* Anda menggunakan kartu ini" atau "simulasikan apa yang akan Anda lakukan jika akun media sosial diretas". Proses *think-aloud* direkam dan dianalisis untuk mengidentifikasi masalah kegunaan (*usability issues*). Kuesioner singkat *System Usability Scale* (SUS) dan wawancara lanjutan digunakan untuk mengukur persepsi kemudahan penggunaan dan niat adopsi. Temuan dari *usability testing* ini menjadi masukan untuk perbaikan iteratif prototipe hingga dihasilkan versi final dari *framework* dan *toolkit*-nya.

3. HASIL DAN PEMBAHASAN

3.1. Temuan Fase Empati dan Definisi (Hasil Analisis Tematik)

Analisis tematik terhadap data wawancara dan FGD menghasilkan empat tema utama yang mendasari perancangan framework:

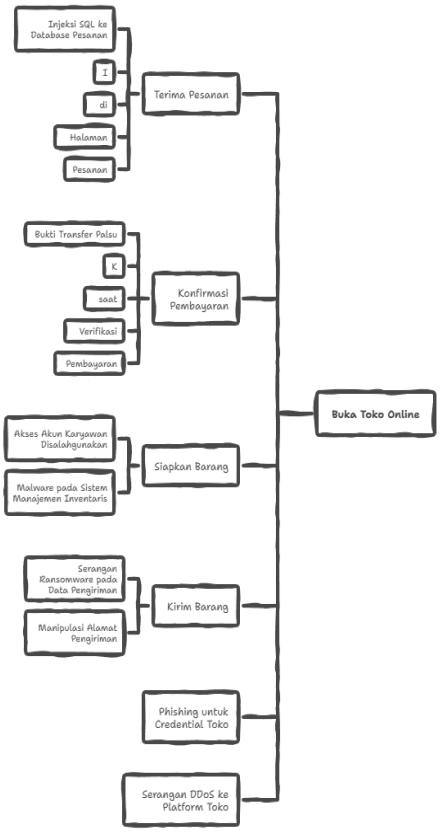
(1) Persepsi Risiko yang Rendah dan Distant ("Bukan Target"): Sebagian besar partisipan (12 dari 15) menganggap ancaman siber sebagai masalah "perusahaan besar" atau "bank". Mereka merasa datanya tidak berharga. Namun, FGD dengan pakar mengungkap bahwa data UMKM justru sangat bernilai untuk identity theft dan serangan ransomware yang mengincar kelancaran operasional.

(2) Kesenjangan Pengetahuan-Praktik yang Lebar: Hampir semua partisipan mengetahui konsep dasar seperti "password yang kuat", tetapi hanya 3 yang secara konsisten menerapkannya untuk semua akun. Alasan utama adalah kebiasaan, kemalasan, dan takut lupa. Ini menunjukkan bahwa pengetahuan saja tidak cukup tanpa intervensi desain yang memudahkan perilaku aman.

(3) Kendala Sumber Daya dan Kerumitan: Solusi keamanan yang dikenal (seperti VPN, anti-virus berbayar) dianggap mahal dan rumit untuk dikonfigurasi. Mereka membutuhkan panduan yang "langsung bisa dipraktekkan" tanpa perlu pemahaman teknis mendalam.

(4) Kontekstualisasi Ancaman: Ancaman paling nyata bagi mereka adalah phishing via WhatsApp dan pesan singkat, penyalahgunaan akun oleh mantan karyawan, dan pembayaran palsu. Ancaman teknis seperti malware kurang dipahami.

Berdasarkan tema-tema ini, dikembangkan dua persona dan user journey map seperti pada Gambar 1.



Gambar 1 Contoh User Journey Map Persona "Budi" dan Titik Kerentanan Siber.

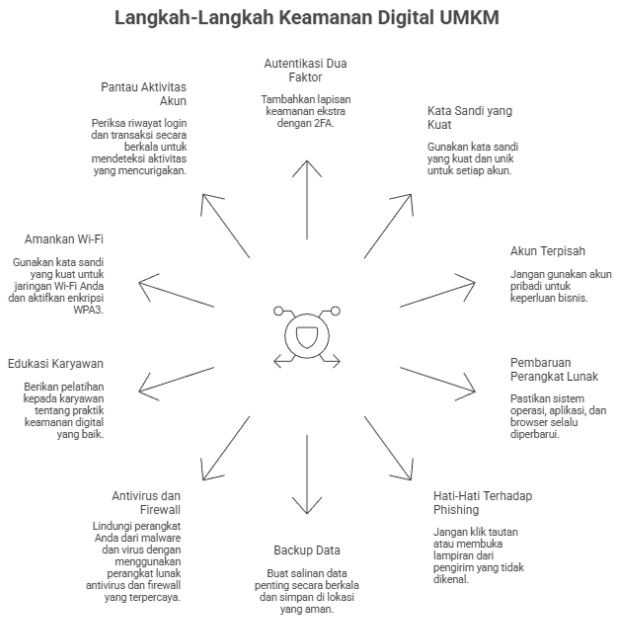
3.2. *Framework* "SIBER UMKM" dan Prototipe *Toolkit*

Framework akhir yang dihasilkan terdiri dari tiga pilar yang saling terkait, yaitu seperti disajikan pada Tabel 1 berikut.

Tabel 1. Pilar *Framework* "SIBER UMKM" dan Komponennya.

Pilar	Tujuan	Contoh Komponen *Toolkit*
Sadari dan pahami	Membangun kesadaran kontekstual	Kartu infografis "5 Ancaman Siber Paling Umum untuk UMKM", video animasi singkat.
Implementasi Higieni Dasar	Mendorong perubahan perilaku praktis	Checklist "10 Langkah Wajib": 1. Gunakan 2FA untuk email & marketplace, 2. Pisahkan akun pribadi & bisnis, dll
Bersiap & Evaluasi	Membangun ketahanan dan respons insiden	*Basic Risk Matrix*, *Flowchart* "Apa yang Harus Dilakukan Jika Diretas?", *Dashboard* monitoring sederhana.
Rujukan & Dukungan	Menyediakan jalur bantuan	Daftar kontak darurat (layanan pengaduan siber), tautan ke panduan resmi.

Prototipe *dashboard* dan kartu *checklist* dirancang dengan prinsip minimalist desain. *Dashboard* menggunakan metafora "Kesehatan Keamanan Digital" dengan indikator warna. Kartu checklist dirancang agar dapat ditempel di dekat *workstation* (Gambar 2).



Gambar 2. Prototipe Kartu Checklist "10 Langkah Wajib Keamanan Digital UMKM"

3.3. Hasil *Usability Testing* dan Refleksi

Usability testing menunjukkan penerimaan yang sangat positif. Skor SUS rata-rata yang diperoleh adalah 82,5, yang tergolong dalam kategori "*Excellent*". Partisipan khususnya menghargai format visual dan bahasa yang langsung ke inti. Tugas prioritisasi risiko menggunakan risk matrix awalnya membingungkan, tetapi setelah diberikan contoh kontekstual (misal: "kehilangan aksen Instagram vs. kehilangan akses rekening bank"), partisipan dapat memahami dan menggunakannya. Niat untuk mengadopsi minimal 7 dari 10 langkah dalam checklist meningkat dari 30% (sebelum intervensi) menjadi 85% (setelah sesi pengujian dan penjelasan).

3.4. Pembahasan

Temuan persepsi risiko rendah konsisten dengan penelitian Ghafur et al. (2020) di UK yang juga menemukan bahwa usaha kecil sering mengabaikan risiko siber karena kurangnya kesadaran akan nilai data mereka. Keunikan penelitian ini adalah mengonversi temuan tersebut menjadi solusi desain yang langsung mengatasi persepsi itu melalui infografis yang menunjukkan nilai konkret data UMKM (misal: "Akses *Marketplace* Anda = Aset Berharga").

Kesenjangan pengetahuan-praktik yang terungkap memperkuat argumen Becker (2021) bahwa intervensi keamanan siber harus bergeser dari sekadar edukasi ke *nudging*—mendorong perilaku yang diinginkan melalui kemudahan desain. *Checklist* dalam penelitian ini berfungsi sebagai nudge dengan menyederhanakan keputusan kompleks menjadi aksi biner (centang/tidak centang).

Pendekatan HCD terbukti efektif dalam menjembatani kesenjangan antara solusi teknis murni dan kebutuhan manusiawi pengguna. Dengan memulai dari *empathy map* dan *user journey, framework* yang dihasilkan tidak hanya mencantumkan kontrol teknis (seperti 2FA), tetapi juga mengakomodasi konteks sosial seperti pengelolaan akses mantan karyawan, yang jarang dibahas dalam panduan konvensional.

Keterbatasan penelitian ini adalah lingkup partisipan yang masih terbatas pada dua sektor dan wilayah geografis tertentu. Pengujian *usability* juga bersifat jangka pendek. Penelitian lanjutan diperlukan

untuk menguji efektivitas jangka panjang *framework* dalam menurunkan insiden keamanan secara aktual dan mengeksplorasi integrasi *toolkit* ke dalam platform digital yang sudah digunakan UMKM, seperti aplikasi akuntansi atau pembukuan digital.

4. KESIMPULAN DAN REKOMENDASI

Penelitian ini berhasil merancang dan mengembangkan sebuah framework keamanan siber tingkat dasar bernama "SIBER UMKM" menggunakan pendekatan *Human-Centered Design. Framework* ini menjawab kebutuhan spesifik UMKM akan panduan yang praktis, visual, dan mudah diadopsi, dengan fokus pada peningkatan *cybersecurity hygiene*. Melalui tahap empati dan definisi, penelitian berhasil mengidentifikasi akar masalah berupa persepsi risiko rendah, kesenjangan pengetahuan-praktik, dan kebutuhan akan solusi kontekstual. Prototipe yang dihasilkan (*dashboard* dan kartu checklist) telah teruji secara *usability* dengan hasil yang sangat baik, menunjukkan potensi tinggi untuk adopsi nyata. Framework ini berkontribusi pada pembangunan ketahanan digital UMKM yang inklusif, sejalan dengan semangat SDG 9.

Berdasarkan temuan, diajukan rekomendasi sebagai berikut:

(1) **Bagi Pemerintah dan Asosiasi:** Mengadopsi dan mengadaptasi framework "SIBER UMKM" ke dalam materi pelatihan dan pendampingan UMKM nasional. *Toolkit* dapat didistribusikan melalui dinas koperasi dan UMKM serta platform digital resmi.

(2) **Bagi Pengembang Layanan UMKM:** Mengintegrasikan prinsip-prinsip dan checklist dari framework ini ke dalam aplikasi atau platform layanan untuk UMKM (e-commerce, akuntansi, logistik) sebagai fitur bawaan untuk menciptakan lingkungan digital yang lebih aman (*secure by design*).

(3) **Bagi Peneliti Selanjutnya:** Melakukan penelitian tindak lanjut untuk mengukur dampak implementasi framework terhadap penurunan insiden keamanan siber pada UMKM secara longitudinal. Juga, mengeksplorasi pengembangan *digital dashboard* interaktif berbasis web atau mobile yang terintegrasi dengan *toolkit* ini.

5. REFERENSI

Alshaikh, M., Maynard, S. B., & Ahmad, A. (2022). *A situational awareness model for cybersecurity in small and medium enterprises*. Computers & Security, 119, 102752. https://doi.org/10.1016/j.cose.2022.102752

Becker, M., Tolsdorf, J., & Lo Iacono, L. (2021). *Nudging towards cybersecurity: A systematic review. ACM Computing Surveys (CSUR)*, 54(8), 1–36. https://doi.org/10.1145/3469883

Braun, V., & Clarke, V. (2006). *Using thematic analysis in psychology. Qualitative Research in Psychology*, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Design Council. (2019). *The Double Diamond: A universally accepted depiction of the design process. Design Council.* https://www.designcouncil.org.uk/our-resources/the-double-diamond/

Ghafur, S., Grass, E., Jennings, N. R., & Darzi, A. (2020). *Cybersecurity in health care: A structured review of the literature. Journal of Medical Internet Research*, 22(10), e21620. https://doi.org/10.2196/21620.