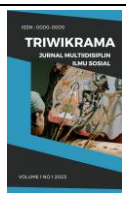
Triwikrama: Jurnal Ilmu Sosial
Volume 11 No 8 2025
E-ISSN: 2988-1986
Open Access:



KEAMANAN SIBER SEBAGAI PILAR BARU KESIAPSIAGAAN RELAWAN: STUDI KASUS SOSIALISASI UKK KSR PMI PT UIN STS JAMBI

Muhammad Faruq Al Mubarok[1], Abdillah Oktavian Syaputra[2], Arya Kamandanu[3]
Fakultas Sains dan Teknologi, Program Studi Sistem Informasi,
Universitas Islam Negeri Sulthan Thaha Saifuddin Jambi

ARTICLE INFO

Article history:
Received November 2025
Revised November 2025
Accepted November 2025
Available online November 2025

Email:
faruqalmubarok1@gmail.com,
abdioktavian67661@gmail.com,
akamandanu440@gmail.com

This is an open access article under the CC BY-SA license.
Copyright © 2025 by Author.

Abstrak

Digitalisasi operasi kemanusiaan meningkatkan efisiensi respons tetapi juga membuka celah ancaman siber yang berdampak langsung terhadap privasi korban, kesinambungan layanan, dan keamanan relawan. Studi kualitatif ini mengevaluasi efektivitas sosialisasi keamanan siber kepada anggota Unit Kegiatan Khusus Korps Sukarela Palang Merah Indonesia Perguruan Tinggi Universitas Islam Negeri Sultan Thaha Saifuddin Jambi (UKK KSR PMI PT UIN STS JAMBI, yang dilaksanakan pada September 2025. Teknik pengumpulan data meliputi observasi partisipatif, wawancara semi-struktural, dokumentasi materi, dan diskusi kelompok kecil. Temuan menunjukkan peningkatan kesadaran praktis terhadap ancaman seperti *phishing*, pengelolaan akses akun (2FA), dan mitigasi risiko berbagi data lapangan; relawan menunjukkan komitmen untuk mengadopsi praktik aman dan merekomendasikan integrasi modul keamanan siber ke kurikulum pelatihan dasar. Hasil ini sejalan dengan bukti literatur bahwa organisasi kemanusiaan menghadapi ancaman digital yang meningkat dan membutuhkan strategi *cyber resilience* yang terintegrasi. Studi ini merekomendasikan (1) penyusunan SOP keamanan data operasional, (2) kapasitas building berkelanjutan (pelatihan berkala dan simulasi), dan (3) kemitraan antara KSR/PMI dan pusat-pusat keamanan siber untuk dukungan teknis dan respons insiden.

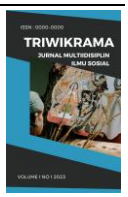
Kata Kunci : Keamanan siber; kesiapsiagaan relawan; KSR PMI; literasi digital; cyber resilience; digital humanitarianism.

Abstract

Digitalization of humanitarian operations enhances response efficiency but simultaneously exposes organizations to cyber threats that directly affect victim privacy, service continuity, and volunteer safety. This qualitative study evaluates the effectiveness of a cybersecurity awareness session delivered to members of the Special Activity Unit of the Volunteer Corps of the Indonesian Red Cross at the State Islamic University Sultan Thaha Saifuddin Jambi (UKK KSR PMI PT UIN STS Jambi) in September 2025. Data collection techniques included participatory observation, semi-structured interviews, documentation of training materials, and small-group discussions. The findings indicate an observable increase in practical awareness of threats such as phishing, account access management (2FA), and risk mitigation related to data sharing in field operations; volunteers expressed commitment to adopting safer practices and recommended integrating cybersecurity modules into the basic training curriculum. These results align with existing literature showing that humanitarian organizations face escalating digital threats and require integrated cyber-resilience strategies. The study recommends (1) developing an SOP for operational data security, (2) implementing continuous capacity building through regular training and simulations, and (3) strengthening partnerships between KSR/PMI units and cybersecurity centers for technical support and incident response.

Keywords *: Cybersecurity; Volunteer Preparedness; Indonesian Red Cross (KSR PMI); Digital Literacy; Cyber Resilience; Digital Humanitarianism.*

Triwikrama: Jurnal Ilmu Sosial
Volume 11 No 8 2025
E-ISSN: 2988-1986
Open Access:



I. PENDAHULUAN

1.1 Latar Belakang

Peran relawan dalam operasi tanggap darurat bencana dan pelayanan kemanusiaan semakin tidak dapat dipisahkan dari penggunaan teknologi digital sebagai alat bantu. Berbagai alat seperti platform komunikasi *Whatsapp*, layanan penyimpanan awan seperti *Google Drive*, hingga aplikasi pemetaan digital digunakan untuk mempercepat koordinasi, memperjelas alur informasi dan meningkatkan efisiensi kerja lapangan dalam melakukan misi pelayanan kemanusiaan. Digitalisasi ini tentu memberikan manfaat yang sangat siginifikan bagi berbagai organisasi dan lembaga kemanusaian, termasuk unit-unit Korps Sukarela Palang Merah Indonesia (KSR PMI), terutama dalam memastikan bahwa informasi kritis dapat diakses dan dibagikan secara cepat selama fase tanggap darurat.

Selain membawa manfaat yang signifikan, pemanfaatan teknologi juga membawa risiko baru terhadap keamanan data dan keberlanjutan operasi pelayanan keamanusiaan. Informasi sensitif seperti data pengungsi dan korban, detail kontak anggota tim, rencana operasi penanganan bencana, serta donasi dapat terekspos jika terjadi insiden keamanan seperti *phishing, malware,* kompromi akun, atau serangan rantai pasok. Laporan global beberapa tahun terakhir menunjukan meningkatnya tren serangan siber yang menarget organisasi nirlaba dan sektor kemanusiaan. Salah satu kasus besar yang menimbulkan dampak luas adalah insiden terhadap Jaringan *Restoring Family Link* milik ICRC/*International Committee Of The Red Cross* pada tahun 2022, yang mana insiden ini menyebabkan gangguan signifikan terhadap layanan pelacakan keluarga akibat pelanggaran keamanan sistem.

Kondisi tersebut menunjukkan pentingnya membangun *cyber resilience*, yaitu kemampuan organisasi untuk mencegah, mendeteksi, merespons, dan pulih dari insiden digital. *Cyber resilience* tidak hanya menjadi kebutuhan teknis semata, tetapi ikut menentukan keberlangsungan pelayanan kemanusiaan. Ketika relawan bekerja dalam situasi darurat, gangguan sistem digital dapat memengaruhi pengambilan keputusan, efektivitas respons, dan kepercayaan publik terhadap lembaga kemanusiaan.

Konteks lokal yang juga memperkuat urgensi penelitian ini adalah hasil pengamatan peneliti pada kegiatan sosialisasi yang diberikan kepada anggota UKK KSR PMI PT UIN STS JAMBI pada 20 September 2025 menunjukkan bahwa meskipun relawan memiliki familiaritas tinggi dalam penggunaan aplikasi komunikasi digital, pemahaman mengenai praktik keamanan informasi dan kebijakan privasi masih terbatas. Tidak adanya pengukuran kuantitatif melalui kuesioner membuat penelitian ini berorientasi pada evaluasi kualitatif terkait dampak sosialisasi, persepsi relawan, serta rekomendasi operasional yang dapat diterapkan pada program peningkatan kapasitas di masa mendatang.

Oleh karena itu, penting untuk menempatkan keamanan siber sebagai salah satu pilar kesiapsiagaan relawan, sejajar dengan kesiapsiagaan medis, psikososial, dan manajemen kebencanaan. Penguatan tata kelola keamanan informasi di tingkat relawan dapat membantu mengurangi risiko kebocoran data, meningkatkan keandalan sistem, serta memperkuat ketahanan organisasi dalam menghadapi dinamika ancaman digital. Kajian teoritis dan temuan empiris dari literatur internasional yang relevan akan digunakan sebagai landasan untuk mendukung urgensi tersebut dan memperkuat argumentasi penelitian ini.

1.2. Rumusan Masalah

1. Bagaimana tingkat pemahaman dan kesadaran relawan UKK KSR PMI PT UIN STS Jambi terhadap praktik keamanan informasi dalam penggunaan alat digital untuk kegiatan tanggap darurat?

2. Apa saja tantangan utama yang dihadapi relawan dalam menerapkan prinsip keamanan siber selama menjalankan tugas kemanusiaan?

3. Bagaimana efektivitas kegiatan sosialisasi keamanan siber dalam meningkatkan wawasan relawan mengenai risiko digital dan langkah mitigasinya?

4. Apa rekomendasi strategis untuk memperkuat cyber resilience di lingkungan relawan UKK KSR PMI PT UIN STS Jambi, khususnya dalam konteks penggunaan teknologi komunikasi dan manajemen data?

1.3. Tujuan Penelitian

1. Mengidentifikasi tingkat pengetahuan, kesadaran, dan persepsi relawan UKK KSR PMI PT UIN STS Jambi terkait risiko keamanan digital dalam aktivitas tanggap darurat.

2. Mendeskripsikan kendala dan potensi kerentanan yang muncul dari penggunaan perangkat serta platform digital oleh relawan.

3. Mengevaluasi kontribusi kegiatan sosialisasi keamanan siber terhadap peningkatan kapasitas relawan dalam memahami dan menerapkan praktik keamanan informasi.

4. Merumuskan rekomendasi operasional dan strategis untuk memperkuat *cyber resilience* relawan sebagai bagian dari kesiapsiagaan organisasi.

II. TINJAUAN PUSTAKA

2.1 *Cyber Resilience* dan Sektor Kemanusiaan

Konsep *cyber resilience* menekankan kemampuan organisasi untuk bertahan terhadap insiden siber melalui proses pencegahan, deteksi, respons, dan pemulihan. Dalam konteks organisasi kemanusiaan yang bergantung pada sistem digital untuk komunikasi dan koordinasi, kerangka ini menjadi sangat penting. Sebagaimana dijelaskan Anderson (2020) dalam *Security Engineering*, ketahanan siber harus dilihat bukan hanya sebagai proteksi teknis, tetapi sebagai "kemampuan sistem untuk terus berfungsi meski berada di bawah tekanan serangan". Hal ini menunjukkan bahwa fokus bukan hanya pada pencegahan, tetapi juga kemampuan adaptasi ketika menghadapi ancaman yang berkembang.

Kendati demikian, berbagai studi menekankan bahwa organisasi kemanusiaan sering mengalami keterbatasan sumber daya, sehingga implementasi keamanan tingkat tinggi menjadi tantangan. Singer dan Friedman (2014) dalam *Cybersecurity and Cyberwar: What Everyone Needs to Know* menegaskan bahwa sektor nirlaba dan kemanusiaan termasuk kelompok paling rentan karena kurangnya tenaga ahli dan minimnya alokasi anggaran dibanding sektor pemerintah atau industri. Faktor tersebut mendorong perlunya strategi keamanan yang disesuaikan konteks, termasuk langkah sederhana, pelatihan dasar, dan kebijakan internal yang realistis.

2.2 Ancaman Khusus untuk Lembaga Kemanusiaan

Ancaman siber terhadap lembaga kemanusiaan memiliki karakteristik yang unik karena data yang dikelola melibatkan populasi rentan, seperti pengungsi dan korban bencana. Serangan seperti *spear-phishing*, ransomware, dan pencurian data menjadi ancaman umum yang dapat mengganggu operasi lapangan. Schneier (2018), dalam bukunya *Click Here to Kill Everybody*, menjelaskan bahwa serangan terhadap lembaga kemanusiaan sering kali bertujuan

mengeksploitasi ekosistem digital yang lemah dan dapat melumpuhkan layanan publik pada skala besar. Hal ini menegaskan bahwa konsekuensi serangan tidak hanya bersifat teknis, tetapi juga berdampak langsung pada keamanan manusia (*human security*).

Selain ancaman langsung, serangan rantai pasok (*supply-chain attacks*) menjadi tantangan berat bagi organisasi kemanusiaan. Ross Anderson (2020) menekankan bahwa ketergantungan terhadap perangkat lunak pihak ketiga membuka celah besar bagi penyerang untuk masuk melalui komponen yang tampak tidak berbahaya. Organisasi kemanusiaan yang menggunakan perangkat gratis atau memiliki pembaruan terbatas menjadi target yang lebih mudah. Kondisi ini menuntut adanya penguatan *governance* teknologi serta kebijakan audit keamanan yang lebih terstruktur.

2.3 Literasi Keamanan dan Efektivitas Pelatihan Keamanan Siber

Pelatihan keamanan siber merupakan salah satu upaya utama untuk mengatasi kelemahan pada faktor manusia dalam ekosistem digital. Buku *The Human Factor in Cybersecurity* oleh Hadnagy (2018) menunjukkan bahwa kesalahan manusia adalah pintu masuk terbesar serangan digital, dan pelatihan yang efektif harus dirancang untuk mengubah perilaku, bukan sekadar menambah pengetahuan. Penelitian lain dalam bidang pendidikan keamanan siber menguatkan bahwa metode interaktif seperti simulasi *phishing* dan studi kasus nyata lebih efektif dibandingkan ceramah satu arah.

Meski demikian, literatur juga menunjukkan bahwa dampak pelatihan sering menurun seiring waktu. Menurut Parsons et al. (2017) dalam *Psychology of Cybersecurity*, pelatihan perlu diperkuat melalui repetisi, pembiasaan, dan kebijakan organisasi yang mendukung perubahan perilaku. Tanpa sistem penguatan (*reinforcement system*), relawan cenderung kembali ke kebiasaan sebelumnya. Hal ini menunjukkan bahwa pelatihan keamanan bagi relawan harus bersifat berkelanjutan dan dikaitkan dengan konteks operasional mereka di lapangan.

2.4 *Digital Humanitarians* dan Etika Data

Kemajuan teknologi digital memberi ruang bagi munculnya *digital humanitarians*, yaitu relawan dan analis yang memanfaatkan data digital untuk mendukung respons bencana. Meier (2015), dalam *Digital Humanitarians*, menjelaskan bagaimana penggunaan crowdsourcing, pemetaan krisis, dan analisis big data mempercepat proses penyelamatan dan pengambilan keputusan. Teknologi ini memungkinkan organisasi kemanusiaan merespons situasi darurat secara lebih cepat dan terkoordinasi, terutama saat berhadapan dengan informasi dalam jumlah besar.

Namun, digitalisasi juga membawa tantangan etika yang kompleks. Slim (2015), dalam *Humanitarian Ethics*, menekankan bahwa pengumpulan dan penggunaan data populasi rentan harus memperhatikan aspek privasi, persetujuan (*informed consent*), dan risiko penyalahgunaan. Selain itu, Floridi dan Taddeo (2016) dalam *The Ethics of Information Warfare* menyoroti bahwa data digital yang bocor dapat menimbulkan ancaman serius bagi keselamatan fisik individu, bukan hanya sekadar pelanggaran privasi. Oleh karena itu, etika data harus menjadi bagian integral dari pelatihan relawan dan kebijakan organisasi agar penggunaan teknologi tetap aman dan bertanggung jawab.

III. METODE PENELITIAN

3.1 Metode Penelitian

Penelitian ini menggunakan pendekatan kualitatif deskriptif, yang bertujuan untuk memahami secara mendalam proses, dinamika, dan hasil dari kegiatan sosialisasi “Keamanan Siber sebagai Pilar Baru Kesiapsiagaan Relawan” di UKK KSR PMI PT UIN STS Jambi. Pendekatan ini dipilih karena penelitian tidak mengukur perubahan perilaku melalui instrumen kuantitatif

seperti pre-test dan post-test, tetapi memfokuskan analisis pada pengalaman, persepsi, pemahaman, dan respons relawan sebelum, ketika, dan setelah menerima sosialisasi.

Menurut Creswell (2018), penelitian kualitatif memungkinkan peneliti menafsirkan fenomena sosial berdasarkan sudut pandang partisipan. Dalam konteks ini, relawan sebagai subjek penelitian dipandang sebagai pemilik pengalaman langsung terkait risiko digital, penggunaan perangkat komunikasi, serta tindak lanjut terhadap materi keamanan siber. Pendekatan kualitatif juga memberi fleksibilitas bagi peneliti untuk menyesuaikan fokus pada temuan lapangan, sehingga memungkinkan hasil penelitian yang lebih kaya dan kontekstual.

Selain itu, penelitian ini menggunakan desain studi kasus *(case study)*. Yin (2018) menjelaskan bahwa studi kasus efektif digunakan ketika peneliti mempelajari fenomena yang terjadi dalam konteks nyata dan ketika batas fenomena dan konteks tidak jelas. Sosialisasi keamanan siber dipandang sebagai suatu kasus tunggal *(single case),* yakni intervensi edukatif yang diberikan kepada relawan KSR sebagai upaya peningkatan kapasitas literasi digital. Dengan demikian, penelitian ini tidak hanya mendeskripsikan kegiatan, tetapi juga mengevaluasi konteks, dinamika partisipan, dan perubahan pemahaman yang muncul setelah kegiatan.

3.2 Lokasi dan Waktu Penelitian

Penelitian ini dilaksanakan di UKK KSR PMI PT UIN STS JAMBI, sebuah unit organisasi kemanusiaan berbasis kampus yang memiliki tugas dan fungsi dalam kegiatan pertolongan pertama, penanggulangan bencana, kesiapsiagaan kampus, serta pelayanan kemanusiaan lainnya.

Lokasi ini dipilih dengan pertimbangan sebagai berikut:

1. Relawan KSR menggunakan berbagai platform digital (*WhatsApp, Google Drive,* dan media sosial lainnya) untuk koordinasi dan komunikasi selama kegiatan atau pelaksanaan tugas.

2. Terdapat kebutuhan peningkatan literasi keamanan siber di lingkungan relawan, mengingat ancaman digital seperti *social engineering*, *phishing,* dan penyalahgunaan data pribadi semakin meningkat.

3. Program sosialisasi keamanan siber ini merupakan kegiatan internal organisasi yang belum pernah diteliti sebelumnya.

Penelitian ini berlangsung selama bulan September 2025, yang mencakup beberapa fase :

1. Fase Persiapan (2 Minggu)
    - Penyusunan rancangan sosialisasi
    - Penyusunan materi sosialisasi
    - Koordinasi dengan pengurus KSR terkait pelaksanaan sosialisasi
2. Fase Pelaksanaan (20 September 2025)
    - Penyampaian materi kepada peserta
    - Diskusi interaktif
    - Observasi respon dan interaksi dengan relawan

3. Fase Pasca Kegiatan (2 Minggu)
    - Wawancara mendalam dengan beberapa peserta
    - Analisis hasil wawancara
    - Penyusunan laporan

3.3 Subjek dan Informan Penelitian

Subjek penelitian adalah anggota aktif UKK KSR PMI PT UIN STS Jambi yang mengikuti sosialisasi keamanan siber. Pemilihan informan menggunakan purposive sampling, yaitu memilih partisipan yang dinilai mampu memberikan informasi relevan berdasarkan pengalaman mereka dalam kegiatan organisasi dan penggunaan platform digital.

3.3.1 Kriteria Informan

1. Anggota aktif, minimal 1 tahun mengikuti kegiatan KSR.
2. Terlibat dalam aktivitas organisasi yang menggunakan perangkat digital.
3. Memiliki smartphone dan menggunakan aplikasi.
4. Mengikuti sosialisasi hingga selesai.
5. Bersedia mengikuti wawancara mendalam.

3.3.2 Jumlah Informan

Dalam penelitian kualitatif, jumlah informan tidak ditentukan secara statistik, melainkan berdasarkan kejenuhan data *(data saturation)*. Informasi dianggap jenuh ketika wawancara tambahan tidak lagi menghasilkan temuan baru.

3.4 Jenis dan Sumber Data

3.4.1 Data Primer

Data primer diperoleh dari :

1. Observasi langsung selama sosialisasi berlangsung, peneliti mencatat:
    - Respon peserta,
    - Keaktifan bertanya,
    - Pemahaman peserta terhadap studi kasus,
    - Interaksi antar-relawan.
2. Wawancara mendalam, digunakan untuk :
    - Mengeksplorasi persepsi relawan tentang keamanan digital,
    - Mengetahui kebiasaan digital partisipan sebelum sosialisasi,
    - Memahami perubahan pemahaman setelah mendapatkan sosialisasi.

3. Catatan lapangan, meliputi:
    - Respon partisipan,
    - Hambatan teknis,
    - Dinamika diskusi,
    - Contoh kejadian yang berkaitan dengan risiko digital.

3.4.2 Data Sekunder

Data sekunder penelitian ini berasal dari :

- Dokumen organisasi (Stuktur, SOP digital, kebijakan komunikasi),
- Modul pelatihan PMI,
- Literatur akademik tentang keamanan siber,
- Pedoman etika data ICRC,
- Artikel ilmiah mengenai literasi digital relawan.

3.5 Teknik Pengumpulan Data

3.5.1 Observasi

Peneliti melakukan observasi selama kegiatan sosialisasi berlangsung untuk mencatat:

- tingkat pemahaman peserta terhadap konsep keamanan siber,
- kemampuan peserta mengidentifikasi ancaman digital,
- antusiasme peserta saat diskusi studi kasus,
- perubahan ekspresi, pertanyaan kritis, dan sikap kehati-hatian digital.

3.5.2 Wawancara

Wawancara dilakukan setelah sosialisasi untuk menggali:

1. Pengalaman relawan dalam menggunakan perangkat digital,
2. Wawasan baru yang diperoleh dari sosialisasi,
3. Perubahan cara berpikir dan praktik keamanan digital,
4. Kebutuhan pelatihan lanjutan.

Model semi-terstruktur dipilih agar peneliti dapat menyesuaikan pertanyaan dengan kondisi lapangan

Triwikrama: Jurnal Ilmu Sosial
Volume 11 No 8 2025
E-ISSN: 2988-1986
Open Access:

3.6 Teknik Analisis Data

Analisis menggunakan model Miles, Huberman, dan Saldana (2014), terdiri dari :

3.6.1 Reduksi Data

Melakukan pemilihan data penting dan menyederhanakan informasi dari wawancara, observasi, dan dokumentasi. Reduksi mencakup:

- identifikasi tema,
- kategorisasi respons peserta,
- penandaan kutipan penting,
- pengelompokan topik seperti ancaman digital, kebiasaan digital, dan pemahaman mitigasi risiko.

3.6.2 Penyajian Data

Penyajian dilakukan melalui:

- Narasi deskriptif,
- Tabel tematik,
- Diagram hubungan antar konsep,
- Kutipan wawancara yang relevan.

Penyajian data bertujuan untuk mempermudah penarikan makna dan melihat pola yang muncul

3.6.3 Penarikan Kesimpulan

Kesimpulan diambil dengan:

- Mencari pola dan hubungan antar temuan,
- Melakukan verifikasi terhadap data wawancara dan observasi,
- Memastikan kesimpulan koheren dengan konteks lapangan.

Kesimpulan tidak bersifat final sejak awal, tetapi dikembangkan secara bertahap selama proses penelitian berlangsung.

IV. HASIL DAN PEMBAHASAN

4.1 Gambaran Umum Pelaksanaan Sosialisasi Keamanan Siber

Sosialisasi dilaksanakan oleh tim peneliti kepada relawan UKK KSR PMI PT UIN STS Jambi sebagai respons atas meningkatnya paparan risiko digital yang muncul dalam aktivitas koordinasi kemanusiaan. Seluruh kegiatan relawan seperti penyebaran informasi donor darah, dokumentasi kegiatan, manajemen inventaris, hingga koordinasi tanggap darurat kini banyak dilakukan melalui platform digital. Perubahan pola kerja ini menciptakan kebutuhan mendesak untuk membangun budaya keamanan digital yang lebih sistematis. Pelaksanaan sosialisasi menggunakan pendekatan pemaparan materi, diskusi kelompok kecil, studi kasus, dan demonstrasi langsung. Peneliti mengobservasi perilaku digital peserta, mencatat respons dan

pertanyaan yang muncul, serta mengumpulkan data melalui diskusi terfokus (FGD) setelah sesi berlangsung. Karena tidak menggunakan pre-test dan post-test, penilaian dilakukan melalui analisis interaksi, keaktifan pertanyaan, perubahan cara pandang, dan pemahaman konseptual peserta.

Hasil observasi menunjukkan bahwa sebagian besar anggota KSR antusias, tetapi tidak memiliki pemahaman formal terkait ancaman keamanan digital. Peserta lebih mengenal penggunaan aplikasi namun belum memahami risiko di balik penggunaannya. Temuan ini sejalan dengan literatur Barton & Kahn (2020), yang menyatakan bahwa organisasi kemanusiaan memiliki tingkat adopsi teknologi tinggi tetapi literasi keamanannya rendah.

4.2 Temuan Kualitatif dari Observasi dan FGD

4.2.1 Kondisis Awal Pemahaman Keamanan Siber

Melalui observasi langsung selama pemaparan materi, peneliti mencatat bahwa peserta menunjukkan perilaku umum yang menandakan kurangnya literasi keamanan digital: penggunaan kata sandi yang sama di berbagai platform, pengabaian verifikasi dua langkah, dan kecenderungan mudah membuka tautan tidak dikenal. Salah satu peserta menyebutkan bahwa ia "sering menerima file dari grup tanpa mengecek sumbernya," yang menunjukkan potensi risiko malware.

FGD mengungkapkan bahwa sebagian besar relawan menganggap keamanan digital bukan prioritas karena "relawan hanya memegang informasi umum." Pemahaman ini menunjukkan kurangnya kesadaran bahwa relawan sering menangani data sensitif seperti nama pengungsi, lokasi posko, nomor telepon keluarga, dan informasi medis dasar. Literatur ICRC (2022) menegaskan bahwa justru informasi kemanusiaan yang tampak sederhana dapat dimanfaatkan pelaku ancaman untuk pola serangan yang lebih besar.

Aspek	Temuan Observasi	Tingkat Risiko
Penggunaan kata sandi	Satu kata sandi digunakan banyak akun	Tinggi
Vertifikasi dua langkah	Mayoritas tidak mengaktifkan	Tinggi
Pengelolaan dokumen	Banyak file dibagikan tanpa enkripsi	Sedang
Kesadaran Phising	Hampir semua peserta tidak mengenali ciri phishing	Tinggi
Pembaruan Aplikasi	Banyak perangkat jarang diperbarui	Sedang - Tinggi

Tabel 4.1 Kondisi Awal Literasi Siber

4.2.2 Peningkatan Pemahaman Melalui Studi Kasus

Materi utama sosialisasi adalah analisis kasus nyata, seperti insiden peretasan *ICRC Restoring Family Links 2022*, serangan ransomware pada lembaga kemanusiaan Afrika (2021), dan kebocoran data koordinasi bencana di Asia Tenggara. Penyajian kasus nyata membuat peserta lebih mudah memahami relevansi keamanan digital dalam konteks kerelawanan.

Selama sesi studi kasus, peserta mulai mengaitkan ancaman digital dengan aktivitas sehari-hari. Beberapa peserta menceritakan pengalaman pribadi menerima pesan

Triwikrama: Jurnal Ilmu Sosial
Volume 11 No 8 2025
E-ISSN: 2988-1986
Open Access:

mencurigakan yang meminta verifikasi WhatsApp atau tautan Google Drive palsu. Diskusi ini menunjukkan peningkatan kemampuan peserta dalam mengidentifikasi pola serangan berbasis rekayasa sosial.

4.3 Analisis Perubahan Pemahaman dan Sikap Keamanan Siber

4.3.1 Indikator Peningkatan Pemahaman

1. Perubahan pola tanya jawab
2. Pernyataan reflektif peserta
3. Partisipasi diskusi

Sebelum Sosialisasi	Sesudah Sosialisasi
Kurang memahami ancaman	Lebih mampu mengidentifikasi
Tidak peduli keamanan	Menganggap keamanan sebagai prioritas
Pasif bertanya	Aktif menganalisis kasus
Tidak paham rekayasa sosial	Mengenali pola phishing dan fraud sosial

Tabel 4.2 Indikator Peningkatan

Pemahaman

4.3.2 Analisis Perubahan Sikap Keamanan Siber

Hasil FGD memperlihatkan perubahan sikap yang cukup kuat, ditandai dengan:

1. Keinginan untuk mengganti kata sandi dan menggunakan manajer kata sandi.
2. Kesadaran bahwa data sensitif dalam melakukan pelayanan kemanusiaan harus dijaga kerahasiaannya.
3. Kesediaan untuk melakukan pelatihan lanjutan.
4. Komitmen untuk membuat SOP keamanan digital internal UKK KSR PMI PT UIN STS JAMBI.

Indikator	Sebelum	Sesudah
Sikap terhadap risiko digitaL	Rendah	Tinggi
Kepatuhan praktik keamanan	Minim	Mulai diterapkan
Kepedulian perlindungan data	Rendah	Meningkat
Kemampuan mengenali ancaman	Lemah	Meningkat signifikan
Inisiatif menerapkan SOP	Tidak ada	Muncul inisiatif

Tabel 4.3 Indikator Perubahan Sikap

Triwikrama: Jurnal Ilmu Sosial
Volume 11 No 8 2025
E-ISSN: 2988-1986
Open Access:

4.4 Keamanan Siber Sebagai Pilar Baru Kesiapsiagaan Relawan

Hasil penelitian memperkuat argumen bahwa keamanan siber merupakan komponen vital dalam kesiapsiagaan relawan. Literasi digital yang rendah menjadikan relawan sebagai titik rentan (*weakest link*) dalam rantai keamanan organisasi. Hal ini relevan dengan teori *Human Factor in Cybersecurity* (Hadlington, 2021) yang menyebutkan bahwa serangan digital 80% dipicu oleh kesalahan manusia, bukan kerentanan teknologi.

Dalam konteks relawan PMI, ancaman digital tidak hanya mengganggu operasional, tetapi juga dapat menimbulkan risiko keselamatan fisik. Kebocoran lokasi posko, data korban, atau nomor kontak medis dapat mengundang eksploitasi pihak tidak bertanggung jawab.

Hasil studi menunjukkan bahwa peningkatan literasi keamanan digital mampu:

1. Meningkatkan kesadaran risiko
2. Memperbaiki perilaku digital
3. Menguatkan ketahanan organisasi terhadap ancaman siber
4. Mengintegrasikan perspektif keamanan ke dalam operasional kerelawanan

Sosialisasi ini menegaskan bahwa literasi keamanan digital harus menjadi bagian kurikulum wajib pelatihan dasar relawan PMI, sejajar dengan manajemen bencana, P3K, dan komunikasi publik.

4.5 Model konseptual Keamanan Siber untuk Relawan KSR

Berdasarkan hasil penelitian, peneliti menyusun rekomendasi model konseptual berikut.

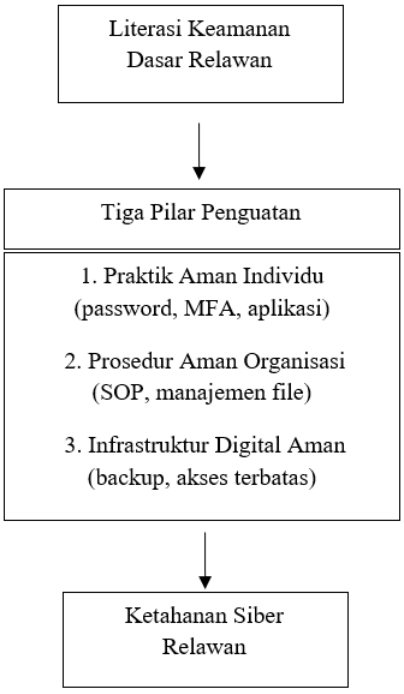


Diagram 4.1 Model Konseptual Pilar Keamanan Siber

4.6 Rangkuman Temuan Utama

1. Literasi keamanan digital relawan awalnya sangat rendah, meskipun penggunaan platform digital sangat tinggi.
2. Sosialisasi berhasil meningkatkan kesadaran, pengetahuan konseptual, dan sikap terhadap keamanan digital.
3. FGD menunjukkan bahwa relawan mulai memahami bahwa keamanan digital merupakan bagian dari perlindungan kemanusiaan.
4. Diperlukan SOP keamanan digital internal UKK KSR PMI agar praktik dapat diterapkan secara berkelanjutan.
5. Temuan memperkuat literatur bahwa keamanan digital harus masuk dalam pilar kesiapsiagaan relawan

V. PENUTUP

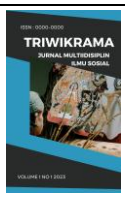
5.1 Kesimpulan

Penelitian ini menunjukkan bahwa keamanan siber merupakan elemen penting dalam kesiapsiagaan relawan, terutama di UKK KSR PMI PT UIN STS Jambi yang sangat bergantung pada perangkat dan platform digital dalam kegiatan operasional. Sosialisasi yang diberikan berhasil meningkatkan pemahaman relawan mengenai ancaman siber yang relevan, seperti phishing, kebocoran data, serta risiko penggunaan aplikasi komunikasi tanpa pengamanan. Meskipun tidak menggunakan metode kuantitatif seperti pre-test dan post-test, hasil observasi dan wawancara menunjukkan adanya perubahan sikap dan praktik digital para relawan, termasuk peningkatan kesadaran terhadap perlindungan data korban dan pentingnya penggunaan autentikasi berlapis. Secara keseluruhan, kegiatan sosialisasi memberikan dampak positif dan menegaskan bahwa keamanan siber perlu dijadikan pilar baru dalam kesiapsiagaan relawan di era digital.

5.2 Saran

Berdasarkan temuan penelitian, UKK KSR PMI PT UIN STS Jambi disarankan untuk memasukkan pelatihan keamanan siber sebagai bagian dari kurikulum wajib relawan serta menyusun SOP keamanan digital yang mencakup pedoman penggunaan aplikasi komunikasi, pengelolaan data sensitif, dan mekanisme pelaporan insiden. Pelatihan berkala dan simulasi ancaman seperti phishing juga perlu dilakukan untuk meningkatkan kesiapsiagaan relawan dalam menghadapi risiko digital yang semakin kompleks. Selain itu, organisasi dianjurkan untuk menerapkan teknologi pendukung seperti autentikasi dua faktor, manajer kata sandi, dan kontrol akses dokumen, serta memastikan adanya edukasi berkelanjutan mengenai etika privasi dan perlindungan data kemanusiaan.

Penguatan budaya keamanan siber juga penting dilakukan melalui kampanye internal dan pengawasan rutin, serta kolaborasi dengan unit keamanan informasi kampus atau PMI Provinsi untuk memperkuat kapasitas teknis. Dokumentasi insiden dan evaluasi berkala perlu dijalankan agar organisasi dapat memahami pola ancaman dan meningkatkan ketahanan siber secara berkelanjutan. Upaya-upaya ini diharapkan mampu menjadikan keamanan digital sebagai pilar baru dalam kesiapsiagaan relawan dan mendukung operasional kemanusiaan yang lebih aman dan responsif



DAFTAR REFERENSI

Marshall, N. (2024). Exploring the evidence for email phishing training: A scoping review. ScienceDirect.

Hillman, D. (2023). Evaluating organizational phishing awareness training on cybersecurity performance. Computers & Security.

Morić, Z. (2025). Evaluating end-user defensive approaches against phishing. MDPI.

Hossain, N. U. (2023). Cyber-susiliency index: A comprehensive resiliency framework. ScienceDirect.

Marelli, M. (2022). The SolarWinds hack: Lessons for international humanitarian organisations. International Review of the Red Cross.

International Committee of the Red Cross (ICRC). (2024). Safeguarding humanitarian organizations from digital threats. ICRC.

CyberPeace Institute. (2024). Cyber-poor, target-rich: Cybersecurity in nonprofit organisations.

Prehospital and Disaster Medicine. (2025). Cybersecurity threats, challenges, and current strategies in humanitarian organizations.

Meier, P. (2015). Digital humanitarians: How big data is changing the face of humanitarian response. CRC Press.

Global Interagency Security Forum (GISF). (2024). Digital security: Humanitarian security in an age of uncertainty.

Ponemon Institute & IBM Resilient. (2020). The cyber resilient organization: Learning to thrive against threats.

UnderServed Project / CyberPeace. (2024). NGO threat landscape report.

Ho, G., et al. (2025). Understanding the efficacy of phishing training in practice. IEEE Symposium on Security and Privacy.

Association for Computing Machinery (ACM). (2024). Embedded phishing training study. ACM Digital Library.