DATA CYBER INDONESIA

Ruang Riset Siber Indonesia

The Orphaned Digital Access Problem: A Cross-Platform Study of Residual Account Access after Employee Turnover in Indonesian MSMEs.

Penulis:

Wijdan manar suriadarma

Peneliti Profesional, Data Cyber Indonesia

Email: wijdanmanarsuriadarma@datacyber.or.id

Website: https://datacyber.or.id

Tanggal Terbit: 12 November 2026

DOI: 10.5281/zenodo.24151071

Lisensi: CC BY 4.0 (Creative Commons Attribution)

Kode Verifikasi: DCY-RISET-2026-028

The Orphaned Digital Access Problem: A Cross-Platform Study of Residual Account Access after Employee Turnover in Indonesian MSMEs.

Abstrak

Transformasi digital telah mendorong pelaku Usaha Mikro, Kecil, dan Menengah (UMKM) di Indonesia untuk menggunakan berbagai platform digital dalam menjalankan aktivitas bisnis. Penggunaan WhatsApp Business, penyimpanan cloud, media sosial, dan marketplace meningkatkan efisiensi operasional, tetapi juga menimbulkan tantangan dalam pengelolaan identitas dan hak akses pengguna.

1. Latar Belakang

Perkembangan teknologi digital telah membawa perubahan besar terhadap aktivitas operasional Usaha Mikro, Kecil, dan Menengah (UMKM) di Indonesia. Saat ini, banyak UMKM memanfaatkan berbagai platform digital, seperti WhatsApp Business, Google Drive, Instagram, marketplace, dan layanan penyimpanan berbasis cloud untuk menjalankan kegiatan bisnis, mengelola pelanggan, menyimpan dokumen, serta melakukan transaksi

2. Rumusan Masalah

Bagaimana mengukur dan menganalisis risiko keberlangsungan akses digital mantan karyawan setelah berakhirnya kewenangan kerja serta mengembangkan model pengukuran Digital Access Residual Lifetime (DARL) untuk meningkatkan keamanan informasi pada UMKM di Indonesia?

3. Tujuan

Penelitian ini bertujuan untuk menganalisis risiko keamanan siber yang timbul akibat masih adanya akun atau hak akses digital mantan karyawan setelah berakhirnya hubungan kerja atau kewenangan dalam suatu UMKM di Indonesia, serta mengembangkan metode pengukuran Digital Access Residual Lifetime (DARL) sebagai pendekatan untuk mengidentifikasi, mengukur, dan mengurangi risiko akses digital yang tidak lagi memiliki kewenangan.

4. Batasan Masalah

Penelitian diarahkan untuk menghasilkan model pengukuran DARL, analisis faktor penyebab keterlambatan pencabutan akses, dan rekomendasi mitigasi risiko

keamanan digital bagi UMKM.
Penelitian tidak dimaksudkan untuk mengukur seluruh jenis serangan siber atau seluruh bentuk kebocoran data di Indonesia.

5. Tinjauan Pustaka

Keamanan siber merupakan serangkaian upaya untuk melindungi sistem komputer, jaringan, aplikasi, dan informasi digital dari akses tidak sah, penyalahgunaan, gangguan, maupun pencurian data.
Dalam konteks penelitian ini, keamanan siber menjadi landasan utama karena permasalahan yang diteliti berkaitan dengan kemungkinan mantan karyawan tetap mempunyai akses terhadap sistem digital perusahaan meskipun kewenangannya telah berakhir.

6. Metodologi

Survei kuantitatif
Target awal 100–150 UMKM dari beberapa wilayah Indonesia.
Wawancara kualitatif
10–15 pemilik usaha atau pengelola sistem digital.
Audit administratif terbatas
Pemeriksaan bukti pencabutan akses dengan izin tertulis, tanpa mencoba masuk ke akun atau sistem tanpa otorisasi.
Analisis data
Statistik deskriptif, perbandingan kelompok, serta analisis hubungan antarvariabel.
Penyusunan model
Menghasilkan indikator DARL dan rekomendasi pengelolaan akses digital.

7. Teknik Analisis

Penelitian menggunakan pendekatan mixed methods dengan:
Statistik deskriptif untuk menggambarkan kondisi akses digital UMKM.
Analisis korelasi untuk mengetahui hubungan antarvariabel.
Analisis regresi untuk menguji faktor yang memengaruhi keterlambatan pencabutan akses.
Analisis tematik untuk mengolah hasil wawancara.
Perhitungan DARL untuk mengukur durasi akses digital tertinggal.

8. Hasil

Hasil yang ditargetkan meliputi identifikasi akun digital yang masih aktif setelah

karyawan berhenti, rata-rata durasi pencabutan akses, faktor penyebab keterlambatan, serta pengembangan model DARL. Hasil aktual akan diisi setelah data dikumpulkan.

9. Pembahasan

Menganalisis hubungan antara kebijakan keamanan informasi, literasi digital, prosedur offboarding, dan risiko akses digital tertinggal. Hasilnya dibandingkan dengan penelitian terdahulu serta standar NIST dan ISO.

10. Kesimpulan

Penelitian diharapkan menghasilkan metode pengukuran DARL untuk mengidentifikasi dan mengevaluasi risiko akses digital mantan karyawan pada UMKM Indonesia.

11. Rekomendasi

UMKM menerapkan prosedur pencabutan akses segera setelah kewenangan berakhir.
Melakukan audit akun secara berkala.
Menggunakan autentikasi multifaktor (MFA).
Menunjuk administrator pengelola akses.
Mengembangkan penerapan model DARL

12. Keterbatasan Riset

Jumlah responden terbatas.
Tidak semua UMKM memiliki dokumentasi akses.
Perbedaan sistem keamanan setiap platform.
Data durasi pencabutan akses mungkin tidak lengkap.
Hasil penelitian tidak otomatis mewakili seluruh UMKM Indonesia.

Daftar Pustaka

NIST. (2020). SP 800-53 Revision 5.
ISO/IEC. (2022). ISO/IEC 27002:2022.
Republik Indonesia. (2022). UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.
NIST. SP 800-61 Revision 3.
OWASP. Employee Lifecycle Security.

Halaman Verifikasi

Dokumen ini diterbitkan secara resmi oleh Data Cyber Indonesia. Pindai QR code di bawah untuk memverifikasi keaslian dokumen ini melalui website kami.

Pindai atau buka tautan berikut untuk memverifikasi:
https://datacyber.or.id/verifikasi/DCY-RISET-2026-028

Kode Verifikasi: DCY-RISET-2026-028

DOI: 10.5281/zenodo.24151071

Lisensi: CC BY 4.0

Diterbitkan oleh Data Cyber Indonesia

Tanggal: 12 November 2026