Jurnal Finansial dan Evaluasi Pasar Modal
Volume: 1, Nomor: 2, Agustus (2026), 150 - 157
Website: https://ejournal.lppnusantara.com/index.php/jfep/article/view/905
EISSN: 3124-7067; DOI: https://doi.org/10.65244/jfep.v1i2.905

ANALISIS TINGKAT LITERASI KEAMANAN SIBER DALAM MENGURANGI RISIKO KEBOCORAN DATA

Zaky Athaillah Hibrizi Nst [1], Muhammad Irwan Padli Nasution [2]
Universitas Islam Negeri Islam Sumatera Utara
Corresponding Author: zaaky1711@gmail.com[1], irwannst@uinsu.ac.id[2]

Info Artikel
Submitted: *04 Mei 2026*
Revised : *09 Juni 2026*
Accepted: *19 Juni 2026*
Published: *25 Juni 2026*

Keywords: *Literacy, Safety, Digital, Cyber*

Abstract
This study aims to analyze the level of cybersecurity literacy in Indonesia and its relationship with data leak risk, using a qualitative approach through literature study (library research) combined with comparative, triangulation, and content analysis techniques. The findings show that cyber threats in Indonesia have reached a critical level, with 3.64 billion attacks recorded in just the first seven months of 2025. Through literature review and secondary data analysis that the author has done, it was found that the human factor is one of the main causes of digital security failures. One example is the cyberattack on the National Data Center (PDN) in 2024, where one of the primary factors behind the breach was human error. Data shows that only 42.7% of the population understands how to manage personal information securely, while the Digital Safety pillar consistently receives the lowest score (3.12 out of 5) in the National Digital Literacy Index. It was also found that every 10% increase in digital privacy literacy can reduce the risk of social impacts resulting from data breaches by 7%. This study concludes that strengthening literacy through formal education, simulation-based training, and strict implementation of the Personal Data Protection Law (PDP Law) regulations is crucial to mitigating the risk of data breaches.

Kata Kunci*: Literasi, Keamanan, Digital, Siber*

Abstrak
Penelitian ini bertujuan untuk menganalisis tingkat literasi keamanan siber di Indonesia serta hubungannya dengan risiko kebocoran data, dengan menggunakan pendekatan kualitatif melalui studi literatur (library research) yang dipadukan dengan teknik perbandingan, triangulasi, dan analisis konten. Temuan menunjukkan bahwa ancaman siber di Indonesia telah mencapai tingkat kritis, dengan 3,64 miliar serangan tercatat hanya dalam tujuh bulan pertama 2025. Melalui kajian literatur dan analisis data sekunder yang telah dilakukan, peneliti menemukan bahwa faktor manusia (human factor) merupakan salah satu faktor utama kegagalan keamanan digital. Salah satu contohnya adalah kasus serangan siber terhadap Pusat Data Nasional (PDN) pada tahun 2024, di mana salah satu faktor utama terjadinya peretasan adalah faktor human error. Data menunjukkan bahwa hanya 42,7% masyarakat yang memahami cara mengelola informasi pribadi dengan aman, sementara pilar Keamanan Digital (Digital Safety) secara konsisten memperoleh skor terendah (3,12 dari 5) dalam Indeks Literasi Digital Nasional. Ditemukan bahwa setiap 10%

peningkatan literasi privasi digital mampu mengurangi risiko dampak sosial akibat kebocoran data sebesar 7%. Penelitian ini menyimpulkan bahwa penguatan literasi melalui pendidikan formal, pelatihan berbasis simulasi, serta implementasi regulasi UU Pelindungan Data Pribadi (UU PDP) secara tegas sangat krusial untuk memitigasi risiko kebocoran data.

Publisher: Lembaga Penerbit Penelitian Nusantara

PENDAHULUAN

Transformasi digital di Indonesia telah mencapai titik di mana ketergantungan masyarakat terhadap layanan digital sangat tinggi. Hal ini mendorong pemerintah untuk beradaptasi dengan membentuk Pusat Data Nasional (PDN) untuk menerapkan sentralisasi data. PDN diharapkan menjadi tulang punggung infrastruktur digital nasional, menyatukan data dari berbagai instansi untuk meningkatkan efisiensi, integrasi, dan keamanan sistem pemerintahan (Bua & Idris, 2025).

Namun, hal ini tidak dibarengi dengan ketahanan siber yang memadai. Pada tahun 2024, PDN justru mengalami serangan siber berupa ransomware yang menyebabkan data nasional tertahan. Hal ini memicu kekhawatiran dan berkurangnya kepercayaan publik terhadap kemampuan instansi pemerintah dalam mengelola data yang krusial. Karena dampaknya terasa luas, mulai dari gangguan layanan publik, potensi penyalahgunaan data pribadi, hingga meningkatnya kecemasan masyarakat akan keamanan digital (Bua & Idris, 2025).

Lemahnya implementasi kebijakan keamanan siber, baik dari aspek teknis maupun regulatif, menjadi salah satu penyebab utama terjadinya kebocoran data nasional. Praktik penggunaan kata sandi yang tidak kuat serta belum diterapkannya standar keamanan minimum yang ketat di berbagai instansi pemerintah membuka peluang bagi peretas untuk melakukan serangan. Di sisi lain, regulasi yang berlaku, termasuk UU ITE dan peraturan turunannya, masih dianggap belum memadai karena kurang spesifik dan tegas dalam mengatur penerapan mekanisme keamanan teknis, seperti autentikasi dua faktor, enkripsi, dan audit keamanan secara berkala. (Bua & Idris, 2025).

Absennya mekanisme penegakan hukum yang tegas, diperparah oleh keterbatasan kapasitas pengawasan, menjadi faktor struktural yang secara langsung memperlemah

ketahanan sistem data nasional. Data terbaru dari Badan Siber dan Sandi Negara (BSSN) menunjukkan adanya 3,64 miliar serangan siber di Indonesia pada semester pertama tahun 2025, di mana 83,68% di antaranya adalah serangan berbasis malware (Tempo.co, 2025). Fakta ini membuat kita menyadari bahwa ancaman siber bukan lagi sekadar potensi, melainkan tantangan nyata yang mengancam stabilitas nasional. Data menunjukkan bahwa meskipun Indeks Literasi Digital Nasional tahun 2022 mengalami kenaikan menjadi 3,54 dari skala 5, pilar Keamanan Digital (*Digital Safety*) secara konsisten memperoleh skor terendah, yakni hanya 3,12 poin (Sanjaya et al., 2024).

Kesenjangan pemahaman ini terlihat dari fakta bahwa hanya 42,7% masyarakat yang memahami cara mengelola informasi pribadi dengan aman di ruang digital. Bahkan, Generasi Z yang dianggap melek teknologi justru menjadi kelompok yang paling abai terhadap protokol keamanan dan perlindungan data pribadi. Untuk mengantisipasi risiko di masa yang akan datang, diperlukan pendekatan edukatif yang dilakukan secara sistematis dan berkesinambungan.

Pelatihan berbasis simulasi situasi nyata (seperti simulasi *anti-phishing* dan *password hygiene*) terbukti jauh lebih efektif dalam meningkatkan keterampilan praktis pengguna dibandingkan sekadar teori. Literasi cybersecurity merupakan fondasi utama dalam menjaga kedaulatan data nasional. Selama masyarakat dan aparatur negara memiliki kesadaran keamanan yang rendah, risiko kebocoran data akan tetap tinggi meskipun didukung oleh infrastruktur teknologi yang canggih.

METODELOGI PENELITIAN

Penelitian mengenai literasi keamanan siber dan kebocoran data ini menggunakan pendekatan kualitatif dengan teknik pengumpulan data berupa metode studi literatur (*library research)* yang dipadukan dengan teknik perbandingan, triangulasi, dan analisis konten. Pendekatan ini digunakan untuk memperoleh gambaran yang holistik dan terperinci untuk memahami bagaimana peran literasi siber dalam memitigasi kebocoran data. Analisis dilakukan secara tematik dan komparatif untuk mengidentifikasi pola kegagalan sistemik dan respons kebijakan pemerintah. Pendekatan kualitatif integratif ini dipilih untuk memperoleh pemahaman holistik yang melampaui data statistik, mencakup dimensi sosial, hukum, dan komunikasi publik dalam ekosistem keamanan siber. Data yang digunakan dalam penelitian ini merupakan data sekunder yang dikumpulkan melalui proses pencarian sistematis dari berbagai sumber otoritatif dan relevan. Sumber data tersebut meliputi jurnal akademik dan hasil

kajian yang merujuk pada penelitian terdahulu mengenai korelasi literasi privasi digital terhadap risiko sosial.

Selain itu, penelitian ini juga menganalisis regulasi dan kebijakan berupa dokumen hukum. Selain itu, penelitian ini turut mengkaji regulasi dan kebijakan yang berbentuk dokumen hukum, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Pelindungan Data Pribadi (UU PDP), serta berbagai kebijakan teknis yang berkaitan dengan keamanan siber dan pengelolaan data. Data tambahan diperoleh dari laporan investigasi resmi yang memuat statistik serangan siber dan indeks literasi digital nasional. Selanjutnya, pemberitaan media massa dari portal berita nasional turut digunakan untuk mendalami narasi serta peristiwa terkini yang berkaitan dengan insiden kebocoran data.

HASIL DAN PEMBAHASAN

1. KONDISI ANCAMAN SIBER DI INDONESIA

Ancaman siber di Indonesia telah sampai pada tingkat yang mengkhawatirkan, di mana Badan Siber dan Sandi Negara (BSSN) mencatat sebanyak 3,64 miliar serangan siber hanya pada semester pertama 2025, angka yang hampir menyamai total anomali selama lima tahun terakhir. Data ini menunjukkan bahwa ancaman serangan siber bukan lagi hanya sebuah potensi, tetapi tantangan nyata yang harus kita hadapi di realitas sekarang yang serba digital.

Meskipun secara internasional Indonesia menempati peringkat keempat dalam keamanan siber di ASEAN, insiden besar seperti peretasan Pusat Data Nasional (PDN) pada tahun 2024 di mana Pusat Data Nasional Sementara (PDNS) pada 20 Juni 2024. PDNS di Surabaya menjadi korban serangan ransomware *Brain Cipher* varian terbaru yang tidak hanya mengganggu layanan keimigrasian, tetapi juga menyebabkan kebocoran data strategis dari Badan Intelijen, TNI, dan POLRI, yang sebagian di antaranya ditemukan dijual di *dark web,* membuktikan bahwa sistem pertahanan nasional masih sangat rentan (Bua & Idris, 2025). Kegagalan sistemik ini sering kali berakar pada kelemahan infrastruktur teknis dan prosedur operasional yang belum matang di berbagai instansi pemerintah.

Serangan tersebut berdampak pada gangguan layanan publik di 210 instansi pemerintahan, dengan Ditjen Imigrasi sebagai yang paling parah terdampak, termasuk lumpuhnya sistem imigrasi di Bandara Soekarno-Hatta dan berbagai kantor imigrasi di seluruh Indonesia (Saputra et al., 2026). Peretas meminta tebusan sebesar US$8 juta (sekitar Rp131 miliar), namun pemerintah menyatakan menolak membayar, sebuah sikap yang mengekspos kelemahan kritis pada ketiadaan *Business Continuity Plan* (BCP) di berbagai instansi pengelola

PDN. Kajian akademis terhadap insiden tersebut mengidentifikasi bahwa penyebab utama kebocoran data terletak pada lemahnya manajemen keamanan, ketiadaan *backup* data, serta buruknya penerapan tata kelola sistem digital secara keseluruhan (Tommy et al., 2025).

2. PROFIL LITERASI KEAMANAN DIGITAL MASYARAKAT INDONESIA

Kesenjangan antara intensitas ancaman dan kapasitas respons masyarakat tergambar jelas dalam data literasi digital nasional. Survei *Status Literasi Digital Indonesia 2022* yang dilakukan Kementerian Komunikasi dan Informatika bekerja sama dengan Katadata Insight Center (KIC) terhadap 10.000 responden di 34 provinsi menghasilkan temuan yang signifikan. Dari empat pilar yang diukur, pilar Keamanan Digital (Digital Safety) secara konsisten menempati skor terendah, yakni 3,12 dari skala 5 di bawah Kecakapan Digital (3,52), Etika Digital (3,68), dan Budaya Digital (3,84).Nilai 3,12 tersebut memiliki implikasi konkret (redaksi siberkreasi, 2023).

Pilar *Digital Safety* mengukur kemampuan pengguna internet dalam mengidentifikasi dan menghapus *spam*/malware/virus di perangkat pribadi, kebiasaan mencadangkan data, serta perlindungan data pribadi di ruang digital. Rendahnya skor ini mengindikasikan bahwa mayoritas pengguna internet Indonesia belum memiliki perilaku keamanan digital yang memadai untuk menghadapi ancaman siber yang terus berkembang.

Kondisi ini diperparah oleh temuan survei APJII 2023 yang mengungkapkan bahwa sebanyak 74,59% masyarakat Indonesia tidak menyadari atau merasa belum pernah mengalami peretasan siber, sementara 10,3% responden melaporkan pernah menjadi korban penipuan *online* dan 7,96% pernah mengalami pencurian data pribadi atau *phishing* (Salwa, 2024). Ketidaksadaran akan risiko ini merupakan faktor yang memperlemah motivasi untuk mengadopsi praktik keamanan digital yang lebih baik.

3. KERENTANAN STRUKTURAL: SEKTOR UMKM

Kelemahan literasi keamanan siber menimbulkan dampak paling nyata di sektor UMKM yang menjadi tulang punggung ekonomi nasional. Penggunaan instrumen Pedoman Penilaian Keamanan Informasi (PAMAN KAMI) yang dikembangkan oleh BSSN berbasis kerangka NISTIR 7621 Rev 1, pengukuran yang dilakukan pada tahun 2020–2022 dengan total 964 UMKM berpartisipasi menunjukkan bahwa hasil penilaian secara konsisten didominasi oleh kategori "Buruk" dan "Kurang". Temuan ini merupakan validasi empiris pertama yang sistematis atas tingkat literasi keamanan informasi UMKM di Indonesia (Ajhari et al., 2022).

Kerentanan UMKM bukan hanya persoalan teknis, melainkan berkakar pada minimnya kesadaran akan risiko. UMKM dengan kebijakan keamanan *email* yang lemah kerap menjadi

korban serangan *phishing*, sementara ketergantungan pada teknologi *cloud* tanpa enkripsi yang memadai dan absennya kebijakan penggunaan perangkat pribadi (BYOD) dalam pekerjaan membuka celah eksploitasi yang signifikan. Data ID-SIRTII juga mengungkap bahwa hanya 28% perusahaan di Indonesia yang memiliki protokol keamanan siber yang memadai.

4. FAKTOR MANUSIA SEBAGAI VARIABEL DETERMINAN

Literatur keamanan siber secara konsisten mengidentifikasi faktor manusia sebagai variabel penentu utama insiden kebocoran data. Penelitian ini menemukan korelasi positif yang kuat (R = 0,72) antara tingkat literasi privasi dengan penurunan risiko dampak sosial akibat kebocoran data. Secara kuantitatif, setiap peningkatan 10% dalam literasi privasi digital mampu mereduksi risiko sosial seperti pencurian identitas dan penyalahgunaan data sebesar 7% (Hakim et al., 2025).

Faktor manusia dinilai krusial dalam konteks pertahanan siber; BSSN secara eksplisit merekomendasikan pelatihan karyawan, simulasi *phishing*, serta verifikasi berlapis untuk transaksi bernilai tinggi sebagai strategi untuk membangun *"human firewall"* yang efektif (ITGID, 2025). Tiga bentuk serangan yang paling sering terjadi dan memanfaatkan kelalaian manusia adalah *ransomware* (penyanderaan data), *phishing* (pencurian kredensial), dan *social engineering* (rekayasa sosial). Praktik dasar yang sering diabaikan, seperti penggunaan kata sandi lemah dan pengabaian fitur autentikasi dua faktor (2FA), menjadi celah utama yang dieksploitasi oleh peretas (Bua & Idris, 2025).

Bukti empiris menunjukkan bahwa metode simulasi situasi nyata jauh lebih efektif dibandingkan edukasi teoretis semata dalam mengubah perilaku keamanan pengguna. BSSN merekomendasikan pelatihan karyawan melalui simulasi *phishing* berkala dan penguatan *password hygiene* sebagai komponen pembangunan *"human firewall"*, didukung oleh kerangka tata kelola seperti COBIT dan ITIL untuk memperkuat resiliensi digital organisasi. Integrasi materi keamanan siber ke dalam kurikulum pendidikan formal dari tingkat dasar hingga perguruan tinggi menjadi keharusan strategis untuk membentuk generasi yang secara alami memiliki budaya keamanan informasi.

Pada level UMKM, pelaksanaan pelatihan berbasis workshop, pendampingan, dan simulasi langsung menggunakan perangkat digital yang dimiliki peserta terbukti menghasilkan peningkatan signifikan dalam kemampuan memahami keamanan digital, pengelolaan data, dan praktik aman dalam transaksi online (Hartanto et al., 2026).

Berlakunya penuh UU PDP sejak 17 Oktober 2024 menandai era baru penegakan hukum perlindungan data di Indonesia. UU ini mengatur sanksi pidana berupa denda maksimal

Rp4–Rp6 miliar dan pidana penjara 4–6 tahun, serta sanksi administratif berupa denda hingga 2% dari pendapatan tahunan bagi pelanggaran ketentuan pemrosesan data. Penyelenggara Sistem Elektronik (PSE) yang mengalami kebocoran data diwajibkan melaporkan insiden kepada regulator dalam waktu 3×24 jam (Simanjuntak, 2024).

Namun, efektivitas UU PDP masih menghadapi hambatan struktural. Hingga Januari 2026, ketidakoptimalan operasional Badan Pelindungan Data Pribadi (Badan PDP) dan masih rendahnya standar enkripsi pada kementerian maupun lembaga pemerintah menjadi hambatan utama dalam pelaksanaan penegakan yang efektif. Hal ini kontras dengan GDPR Uni Eropa yang menetapkan denda hingga 20 juta euro atau sebesar 4% dari total pendapatan tahunan global. UU PDP menetapkan denda maksimal 2% dengan penekanan lebih pada sanksi pidana, sebuah pendekatan yang mencerminkan karakteristik hukum nasional Indonesia.

KESIMPULAN

Temuan penelitian ini secara kolektif menegaskan bahwa ketahanan siber nasional tidak dapat sepenuhnya dibangun di atas kecanggihan infrastruktur teknologi tanpa dibarengi budaya keamanan informasi yang tertanam di setiap lapisan masyarakat. Angka 3,64 miliar serangan dalam tujuh bulan pertama 2025 menjadi alarm serius bagi seluruh instansi pemerintahan dan pelaku sektor privat, sementara skor literasi keamanan digital yang stagnan di 3,12 mencerminkan urgensi intervensi sistemis yang tidak dapat ditunda lebih lama.

Korelasi kuat antara peningkatan literasi privasi dan penurunan risiko kebocoran data (R = 0,72) membuktikan bahwa investasi pada sumber daya manusia memiliki dampak terukur yang signifikan. Setiap kenaikan 10% literasi privasi digital berpotensi mereduksi risiko pencurian identitas dan penyalahgunaan data sebesar 7%, sebuah temuan yang seharusnya menjadi landasan kebijakan nasional yang konkret.

Sinergi antara pemerintah sebagai regulator, sektor swasta sebagai pengelola sistem, dan masyarakat sebagai subjek aktif pelindungan data adalah prasyarat mutlak untuk membangun ekosistem digital yang aman dan berdaulat. Selama faktor manusia tetap menjadi titik terlemah dalam rantai keamanan siber, risiko kebocoran data akan terus menjadi ancaman eksistensial bagi stabilitas dan kedaulatan data nasional Indonesia.

DAFTAR PUSTAKA

Ajhari, A. A., Manaon, M. A., Priambodo, D. F., Bidang, D., Siber, K., Siber, B., Bidang, D., Siber, K., & Siber, B. (2022). *Security Awareness Framework untuk Usaha Mikro ,*

Kecil dan Menengah di Indonesia. (1), 1–7.

Bua, I. T., & Idris, N. I. (2025). *Analisis Kebijakan Keamanan Siber di Indonesia : Studi Kasus Kebocoran Data Nasional pada Tahun 2024*. *2*, 100–114.

Hakim, A. S., Mustaqim, P. J., & Karom, A. N. (2025). *The Role of Digital Education in Protecting User Privacy and Preventing Social Impact*. *4*(2), 162–174.

Hartanto, M. B., Nugroho, Y. C., Fahurian, F., & Yunita, H. D. (2026). *Jurnal Pengabdian Ilmu Komputer Universitas Lampung*. *04*(01), 9–16.

redaksi siberkreasi. (2023, February 11). Status Literasi Digital Indonesia Tahun 2022 Naik. *Siberkreasi*. https://gnld.siberkreasi.id/status-literasi-digital-indonesia-pada-tahun-2022-naik-termasuk-kategori-sedang/

Salwa, N. D. K. (2024, November 18). Tantangan & Hambatan Besar yang Dihadapi CSIRT-BSSN Indonesia. *CSIRT Indonesia*. https://csirt.or.id/pengetahuan-dasar/tantangan-csirt-bssn

Sanjaya, S., Fitriati, L. R., Hakim, M. A., Yasin, M. Y., & Maesaroh, S. S. (2024). *Analisis Literasi Keamanan Digital Bagi Mahasiswa Universitas Pendidikan Indonesia Kampus Tasikmalaya : 4*, 8205–8216.

Saputra, T., Yuharian, R. A., Akbar, M. I., & Elfina, A. (2026). *Analisis Kronologi dan Penanganan Insiden Ransomware pada PDNS 2 Sebagai Evaluasi Strategi Keamanan Data Pemerintah Indonesia*. *3*(8), 2305–2309.

Simanjuntak, P. H. (2024). *Perlindungan Hukum Terhadap Data Pribadi pada Era Digital di Indonesia : Studi Undang-Undang Perlindungan Data Pribadi dan General Data Protection Regulation (GDPR)*. *6*(2), 105–124. https://doi.org/10.17933/mti.v9i1.118

Tempo.co. (2025, August 8). BSSN Catat 3,64 Miliar Serangan Siber di Indonesia Setengah Tahun Ini. *TEMPO*. https://www.tempo.co/digital/bssn-catat-3-64-miliar-serangan-siber-di-indonesia-setengah-tahun-ini-2056396

Tommy, S., Irwan, M., & Nasution, P. (2025). *Evaluasi Manajemen Risiko Keamanan Siber pada Infrastruktur Digital Pemerintah : Studi Kasus Pusat Data Nasional (PDN)*. *3*(6), 330–346.