Original Article

e-XXXX-XXXX

Original Article

Analisis Keamanan Sistem Informasi terhadap Ancaman Data Leakage Melalui Human Error

Fitra Ramadhani[1]✉, Zaskiah Nurul Hikmah [2] , Muhammad Dzacky Putra Alena[3], Rakhmadi Rahman[4]

[1,2,3]Institut Teknologi Bacharuddin Jusuf Habibie, Parepare, Indonesia,

Korespondensi Author: fitraramadhani.241031112@mahasiswa.ith.ac.id, zaskiahnurulhikmah.241031103@mahasiswa.ith.ac.id, muhammaddzackyputraalena.241031105@mahasiswa.ith.ac.id, rakhmadi.rahman@ith.ac.id

Abstrak:

Kebocoran data (data leakage) merupakan salah satu ancaman paling krusial terhadap keamanan sistem informasi dan sering kali tidak hanya disebabkan oleh celah teknis, tetapi juga oleh kesalahan manusia (human error). Penelitian ini bertujuan untuk menganalisis peran human error dalam terjadinya kebocoran data serta mengevaluasi langkah-langkah pencegahan yang dapat diterapkan pada sistem informasi organisasi. Metode penelitian yang digunakan adalah pendekatan deskriptif kualitatif melalui studi literatur, analisis kasus insiden kebocoran data, serta pemetaan faktor human error menggunakan kerangka People–Process–Technology (PPT). Hasil penelitian menunjukkan bahwa bentuk human error yang paling umum meliputi penggunaan kata sandi yang lemah, kesalahan pengiriman data, kerentanan terhadap phishing, serta kesalahan konfigurasi hak akses. Kesalahan-kesalahan tersebut secara signifikan meningkatkan risiko kebocoran data meskipun sistem telah dilengkapi dengan kontrol keamanan teknis. Penelitian ini menyimpulkan bahwa mitigasi yang efektif memerlukan kombinasi antara peningkatan kesadaran keamanan pengguna, penerapan prosedur operasional standar yang jelas, serta pemantauan berkelanjutan yang didukung oleh kontrol teknis seperti manajemen akses dan sistem pencegahan kebocoran data.

Keywords: Keamanan Sistem Informasi, Kebocoran Data, Human Error, Kesadaran Keamanan, Mitigasi Risiko.

Pendahuluan

Perkembangan teknologi informasi dan komunikasi telah mendorong organisasi untuk mengelola data dalam jumlah besar secara digital. Data tidak hanya berfungsi

Received: November 17, 2025 – Revised: November 30, 2025 - Accepted: Desember 19, 2025 - Published online: January 10, 2026

sebagai sumber informasi, tetapi juga menjadi aset strategis yang menentukan keberlangsungan operasional serta daya saing organisasi (Whitman & Mattord, 2021). Seiring dengan meningkatnya ketergantungan terhadap sistem informasi, ancaman terhadap keamanan data juga mengalami peningkatan, baik dari segi kompleksitas maupun dampaknya.

Salah satu ancaman keamanan data yang paling serius adalah kebocoran data (data leakage), yaitu kondisi ketika data sensitif diakses, disebarkan, atau berpindah ke pihak yang tidak berwenang, baik secara sengaja maupun tidak disengaja (Solove & Schwartz, 2020). Berbagai penelitian menunjukkan bahwa kebocoran data tidak selalu disebabkan oleh kegagalan teknologi, melainkan sering kali dipicu oleh faktor manusia (human error) (ENISA, 2023). Laporan Verizon Data Breach Investigations Report (2023) juga mengungkapkan bahwa faktor manusia memberikan kontribusi signifikan terhadap sebagian besar insiden pelanggaran data yang terjadi secara global.

Human error dalam konteks keamanan sistem informasi mencakup berbagai bentuk kelalaian, kurangnya pemahaman terhadap prosedur keamanan, serta kesalahan dalam pengambilan keputusan oleh pengguna maupun administrator sistem. Contoh human error antara lain penggunaan kata sandi yang lemah, ketidaksengajaan dalam membagikan data sensitif, serta rendahnya kewaspadaan terhadap serangan rekayasa sosial seperti phishing (Anderson, 2020). Kesalahan-kesalahan tersebut kerap terjadi meskipun organisasi telah menerapkan kontrol keamanan teknis yang memadai.

Kondisi ini menunjukkan bahwa pendekatan keamanan sistem informasi yang hanya berfokus pada aspek teknologi tidak lagi mencukupi. Diperlukan pendekatan yang lebih komprehensif dengan mempertimbangkan keterkaitan antara manusia, proses, dan teknologi secara terpadu (Pfleeger & Pfleeger, 2019). Oleh karena itu, penelitian ini menjadi relevan untuk mengkaji secara mendalam peran human error dalam terjadinya kebocoran data serta merumuskan strategi mitigasi yang efektif.

Berdasarkan latar belakang tersebut, tujuan penelitian ini adalah: (1) mengidentifikasi bentuk-bentuk human error yang berkontribusi terhadap kebocoran data; (2) menganalisis dampak human error terhadap keamanan sistem informasi; dan (3) merumuskan strategi mitigasi yang dapat diterapkan untuk meminimalkan risiko data leakage akibat faktor manusia.

Metode

PPenelitian ini menggunakan metode deskriptif kualitatif dengan pendekatan studi literatur dan analisis konseptual. Data penelitian diperoleh dari berbagai sumber, antara lain jurnal ilmiah, laporan insiden keamanan, standar keamanan informasi, serta publikasi resmi yang berkaitan dengan kasus kebocoran data.

Tahapan penelitian dilakukan secara sistematis. Tahap pertama adalah mengidentifikasi insiden kebocoran data yang disebabkan oleh faktor human error berdasarkan kajian literatur dan laporan keamanan yang relevan. Tahap kedua yaitu mengklasifikasikan jenis-jenis human error menggunakan kerangka People–Process–Technology (PPT) untuk memahami keterkaitan antara faktor manusia, proses, dan teknologi. Tahap ketiga adalah menganalisis dampak dari setiap jenis human error terhadap aspek keamanan data, yaitu kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*). Tahap terakhir adalah merumuskan strategi mitigasi berdasarkan praktik terbaik (best practices) dalam keamanan sistem informasi.

Analisis data dilakukan secara kualitatif dengan tujuan untuk menggambarkan hubungan antara faktor manusia dan risiko kebocoran data, serta mengevaluasi

Received: November 17, 2025 – Revised: November 30, 2025 - Accepted: Desember 19, 2025 - Published online: January 10, 2026

efektivitas upaya pengendalian yang dapat diterapkan. Pendekatan ini diharapkan mampu memberikan pemahaman yang komprehensif mengenai peran human error dalam terjadinya kebocoran data serta solusi yang dapat digunakan untuk meminimalkan risiko tersebut.

Hasil dan Pembahasan

Identifikasi Bentuk Human Error Penyebab Data Leakage

Hasil kajian literatur dan analisis konseptual menunjukkan bahwa *human error* merupakan salah satu faktor dominan dalam insiden kebocoran data. Menurut laporan ENISA (2023), lebih dari 60% insiden keamanan informasi melibatkan kesalahan manusia baik secara langsung maupun tidak langsung. *Human error* dalam konteks keamanan sistem informasi dapat dipahami sebagai tindakan atau kelalaian pengguna yang menyimpang dari prosedur keamanan yang telah ditetapkan (Sasse et al., 2001).

Bentuk *human error* yang paling sering ditemukan meliputi penggunaan kata sandi yang lemah dan berulang (Anderson, 2020), kesalahan pengiriman dokumen sensitif ke pihak yang tidak berwenang, serta kurangnya kewaspadaan terhadap serangan rekayasa sosial seperti phishing dan spear phishing (Verizon, 2023). Selain itu, kesalahan konfigurasi hak akses oleh administrator sistem juga termasuk dalam kategori *human error* yang berisiko tinggi terhadap data leakage (ISO/IEC, 2022).

Tabel 1. Klasifikasi Human Error Penyebab Data Leakage

No	Jenis Human Error	Deskripsi	Dampak terhadap Keamanan
1	Kata sandi lemah	Penggunaan kata sandi sederhana, berulang, atau dibagikan	Akses tidak sah dan pelanggaran kerahasiaan data
2	Kesalahan pengiriman data	Data sensitif dikirim ke pihak yang tidak berwenang	Kebocoran informasi organisasi
3	*Phishing* & rekayasa sosial	Pengguna tertipu email atau tautan palsu	Pengambilalihan akun dan pencurian data
4	Salah konfigurasi hak akses	Hak akses berlebih atau tidak diperbarui	Eksposur data internal

Tabel ini menyajikan klasifikasi bentuk-bentuk human error yang paling sering menjadi penyebab terjadinya kebocoran data. Hasil kajian literatur menunjukkan bahwa kelemahan perilaku pengguna, seperti penggunaan kata sandi yang tidak aman dan kurangnya kewaspadaan terhadap serangan phishing, menjadi faktor dominan dalam insiden data leakage. Kesalahan ini dapat terjadi baik pada level pengguna akhir maupun administrator sistem dan berimplikasi langsung pada pelanggaran keamanan informasi.

Untuk memperoleh gambaran yang lebih sistematis, bentuk-bentuk human error tersebut kemudian dipetakan menggunakan kerangka People–Process–Technology (PPT) sebagaimana ditunjukkan pada Tabel 2.

Tabel 2. Pemetaan *Human Error* Berdasarkan Kerangka People, Process dan Technology (PPT)

Received: November 17, 2025 – Revised: November 30, 2025 - Accepted: Desember 19, 2025 - Published online: January 10, 2026

Aspek PPT	Bentuk Human Error	Contoh Kasus
People	Kurangnya kesadaran keamanan	Pengguna mengklik tautan phishing
Process	SOP keamanan tidak jelas	Tidak ada prosedur klasifikasi data
Technology	Kesalahan konfigurasi sistem	Hak akses admin berlebihan

Berdasarkan kerangka People–Process–Technology (PPT), human error tidak hanya disebabkan oleh individu, tetapi juga oleh kelemahan proses dan konfigurasi teknologi. Tabel ini menunjukkan bahwa pendekatan keamanan sistem informasi harus bersifat holistik. Tanpa dukungan proses yang jelas dan teknologi yang dikonfigurasi dengan benar, kesalahan manusia akan terus menjadi celah keamanan yang signifikan.

Dampak Human Error terhadap Keamanan Sistem Informasi

Human error berdampak signifikan terhadap tiga pilar utama keamanan informasi, yaitu kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability). Kesalahan pengguna dalam menjaga kredensial dapat menyebabkan akses tidak sah terhadap data sensitif, sehingga melanggar prinsip kerahasiaan (Whitman & Mattord, 2021)whit. Dari sisi integritas, kesalahan input atau manipulasi data tanpa validasi yang memadai dapat mengakibatkan perubahan data yang tidak terdeteksi.

Tabel 3. Dampak Human Error terhadap Pilar Keamanan Informasi (CIA Triad)

Jenis *Human Error*	*Confidentiality*	*Integrity*	*Availability*
Password lemah	✓	–	–
Phishing	✓	✓	–
Salah hak akses	✓	✓	–
Kesalahan penghapusan data	–	–	✓

Tabel ini menggambarkan hubungan antara human error dan tiga pilar utama keamanan informasi, yaitu kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability). Hasil analisis menunjukkan bahwa sebagian besar kesalahan manusia berdampak langsung pada aspek kerahasiaan data, sedangkan kesalahan operasional tertentu juga dapat memengaruhi integritas dan ketersediaan sistem.

Dampak lanjutan dari kebocoran data akibat human error tidak hanya bersifat teknis, tetapi juga organisatoris dan hukum. Organisasi dapat mengalami kerugian finansial, gangguan operasional, serta sanksi hukum akibat pelanggaran regulasi perlindungan data (GDPR maupun UU PDP di Indonesia) sebagaimana dijelaskan oleh Solove dan Schwartz (2020).

Strategi Mitigasi dan Pengendalian Risiko

Mitigasi risiko data leakage akibat human error memerlukan pendekatan holistik yang mencakup aspek manusia, proses, dan teknologi. Pelatihan kesadaran keamanan (security awareness training) secara berkelanjutan terbukti mampu menurunkan tingkat keberhasilan serangan phishing hingga 70% (ENISA, 2023). Selain itu, penerapan kebijakan keamanan yang jelas dan mudah dipahami dapat meningkatkan kepatuhan pengguna terhadap prosedur yang berlaku (Pfleeger & Pfleeger, 2019).

Received: November 17, 2025 – Revised: November 30, 2025 - Accepted: Desember 19, 2025 - Published online: January 10, 2026

Tabel 4. Strategi Mitigasi Data Leakage Akibat Human Error

No	Strategi Mitigasi	Pendekatan	Manfaat
1	*Security awareness training*	*People*	Mengurangi kesalahan pengguna
2	SOP keamanan data	*Process*	Meningkatkan kepatuhan
3	Autentikasi multifaktor	*Technology*	Mengurangi risiko akses ilegal
4	*Data Loss Prevention* (DLP)	*Technology*	Mencegah kebocoran data
5	Audit & *monitoring* berkala	*Process & Technology*	Deteksi dini insiden

Strategi mitigasi yang efektif terhadap data leakage akibat human error memerlukan kombinasi pendekatan manusia, proses, dan teknologi. Tabel ini menunjukkan bahwa pelatihan kesadaran keamanan perlu didukung oleh kebijakan yang jelas serta kontrol teknis seperti autentikasi multifaktor dan DLP. Pendekatan berlapis ini terbukti mampu menurunkan risiko kebocoran data secara signifikan.

Dari sisi teknis, penerapan autentikasi multifaktor, prinsip least privilege, serta sistem Data Loss Prevention (DLP) berperan penting dalam meminimalkan dampak kesalahan manusia (Behl & Behl, 2017). Pengawasan berkelanjutan melalui audit keamanan dan logging aktivitas pengguna juga direkomendasikan untuk mendeteksi potensi kebocoran data sejak dini (NIST, 2020).

Kesimpulan

Berdasarkan hasil analisis yang telah dilakukan, dapat disimpulkan bahwa kebocoran data (data leakage) tidak hanya disebabkan oleh kelemahan teknis pada sistem informasi, tetapi juga sangat dipengaruhi oleh faktor manusia (human error). Penelitian ini menunjukkan bahwa bentuk human error yang paling sering berkontribusi terhadap kebocoran data meliputi penggunaan kata sandi yang lemah, kesalahan dalam pengiriman data, kerentanan terhadap serangan phishing, serta kesalahan konfigurasi hak akses.

Hasil penelitian juga mengungkapkan bahwa keberadaan kontrol keamanan teknis saja belum cukup untuk mencegah terjadinya kebocoran data. Tanpa didukung oleh kesadaran keamanan pengguna dan penerapan prosedur yang jelas, sistem informasi tetap rentan terhadap eksploitasi yang berasal dari kesalahan manusia. Oleh karena itu, pendekatan keamanan yang komprehensif dengan mengintegrasikan aspek manusia, proses, dan teknologi menjadi kebutuhan yang sangat penting dalam upaya perlindungan data organisasi.

Saran

Berdasarkan hasil penelitian yang telah dilakukan, disarankan agar organisasi meningkatkan kesadaran keamanan informasi bagi seluruh pengguna sistem melalui pelatihan dan edukasi keamanan secara berkala. Selain itu, organisasi perlu menetapkan dan menerapkan prosedur operasional standar yang jelas terkait pengelolaan data dan akses sistem guna meminimalkan potensi kesalahan manusia.

Disarankan pula untuk memperkuat kontrol teknis dengan menerapkan manajemen akses berbasis prinsip least privilege, autentikasi berlapis, serta sistem pencegahan kebocoran data (Data Loss Prevention). Penelitian selanjutnya diharapkan

Received: November 17, 2025 – Revised: November 30, 2025 - Accepted: Desember 19, 2025 - Published online: January 10, 2026

dapat mengkaji secara empiris efektivitas kombinasi strategi mitigasi tersebut pada berbagai jenis organisasi dan lingkungan sistem informasi yang berbeda, sehingga diperoleh model mitigasi kebocoran data yang lebih optimal dan aplikatif.

Daftar Pustaka

Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems (3rd ed.). Wiley.

Behl, A., & Behl, K. (2017). Cyberwar: The Next Threat to National Security and What to Do About It. Oxford University Press.

ENISA. (2023). Human Error and Cybersecurity Incidents. European Union Agency for Cybersecurity.

ISO/IEC. (2022). Information Security Management Systems – Requirements. ISO.

NIST. (2020). Security and Privacy Controls for Information Systems and Organizations (SP 800-53 Rev. 5). National Institute of Standards and Technology.

Pfleeger, C. P., & Pfleeger, S. L. (2019). Security in Computing (5th ed.). Pearson.

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the weakest link: A human/computer interaction approach to usable and effective security. BT Technology Journal, 19(3), 122–131.

Solove, D. J., & Schwartz, P. M. (2020). Information Privacy Law. Wolters Kluwer.

Verizon. (2023). Data Breach Investigations Report. Verizon Enterprise.

Whitman, M. E., & Mattord, H. J. (2021). Principles of Information Security (7th ed.). Cengage Learning.

Received: November 17, 2025 – Revised: November 30, 2025 - Accepted: Desember 19, 2025 - Published online: January 10, 2026