Manajemen Kreatif Jurnal
Volume 3, Nomor 1, Tahun 2025
E-ISSN: 2963-9654 dan P-ISSN: 2963-9638, Hal 01-09
DOI: https://doi.org/10.55606/makreju.v3i1.3557
Available Online at: https://ejurnal.stie-trianandra.ac.id/index.php/makreju

Efektivitas Manajemen Risiko Sumber Daya Manusia dalam Menghadapi Risiko Keamanan Data Karyawan di Sektor Teknologi

Ridho Alfi Fajar Hidayat[1*], M. Rafli Lingga[2], Rushel Hardi[3], Abdul Haris Veriyadna[4], Arsyadona Arsyadona[5]
[1-5]Fakultas Ekonomi dan Bisnis Islam, Universitas Islam Negeri Sumatera Utara, Indonesia
Email : ridhoalfifajar@gmail.com[1], raflilingga14@gmail.com[2], rushelhardi@gmail.com[3], harisveriyadna@gmail.com[4], arsyadona1100000174@uinsu.ac.id[5]*

Alamat : Jl. William Iskandar Ps. V, Medan Estate, Kec. Percut Sei Tuan, Kabupaten Deli Serdang, Sumatera Utara 20371
Korespondensi penulis : ridhoalfifajar@gmail.com

Abstract: *This research aims to explore the effectiveness of human resource risk management in dealing with employee data security risks in the technology sector. Given the increasing threats to information security, especially in today's digital age, this research uses a qualitative approach with systematic literature analysis of various related articles and studies. The results show that the existence of clear security policies and procedures, regular employee training, the use of appropriate technology, and an organizational culture that supports information security are key factors that influence the effectiveness of risk management. In addition, evaluation and gathering feedback from employees are important elements in adjusting policies to meet evolving security challenges. This research provides recommendations for companies in the technology sector to improve their risk management systems through the integration of comprehensive policies, effective training programs, and the implementation of advanced technology, in order to protect employee data and increase trust within the organization.*

Keywords: *Risk, Management, Data, Security, Organization.*

Abstrak: Penelitian ini bertujuan untuk mengeksplorasi efektivitas manajemen risiko sumber daya manusia dalam menghadapi risiko keamanan data karyawan di sektor teknologi. Mengingat meningkatnya ancaman terhadap keamanan informasi, terutama di era digital saat ini, penelitian ini menggunakan pendekatan kualitatif dengan analisis literatur sistematis dari berbagai artikel dan studi terkait. Hasil penelitian menunjukkan bahwa keberadaan kebijakan dan prosedur keamanan yang jelas, pelatihan karyawan yang rutin, penggunaan teknologi yang tepat, serta budaya organisasi yang mendukung keamanan informasi merupakan faktor-faktor kunci yang mempengaruhi efektivitas manajemen risiko. Selain itu, evaluasi dan pengumpulan umpan balik dari karyawan menjadi elemen penting dalam penyesuaian kebijakan untuk menghadapi tantangan keamanan yang terus berkembang. Penelitian ini memberikan rekomendasi bagi perusahaan di sektor teknologi untuk meningkatkan sistem manajemen risiko mereka melalui integrasi kebijakan yang komprehensif, program pelatihan yang efektif, dan penerapan teknologi yang canggih, guna melindungi data karyawan dan meningkatkan kepercayaan di dalam organisasi.

Kata Kunci: Manajemen, Risiko, Keamanan, Data, Organisasi.

1. PENDAHULUAN

Dalam era digital yang semakin berkembang pesat, keamanan data karyawan di sektor teknologi menjadi perhatian utama bagi perusahaan. Data karyawan, yang mencakup informasi pribadi, finansial, dan rekam jejak profesional, sangat rentan terhadap ancaman keamanan, termasuk peretasan, kebocoran data, dan penyalahgunaan informasi. Perusahaan di sektor ini menghadapi tantangan untuk melindungi data karyawan secara efektif, terutama di tengah meningkatnya jumlah serangan siber yang kian kompleks dan terstruktur. Risiko ini dapat merugikan perusahaan secara finansial dan merusak reputasi jika tidak dikelola

Received Oktober 23, 2024; Revised November 20, 2024; Accepted Desember 22, 2024; Online Available: Desember 24, 2024

dengan baik. Oleh karena itu, implementasi manajemen risiko sumber daya manusia (SDM) yang efektif diperlukan untuk mengidentifikasi, menganalisis, dan mengurangi risiko keamanan data karyawan dalam perusahaan teknologi.

Permasalahan yang dihadapi oleh mitra penelitian ini, yaitu perusahaan teknologi di Indonesia, antara lain: (1) terbatasnya protokol keamanan yang diterapkan untuk melindungi data karyawan, (2) kesadaran yang masih rendah di kalangan karyawan mengenai pentingnya keamanan data, (3) sistem pengelolaan data karyawan yang belum optimal, sehingga berpotensi menimbulkan kebocoran data, dan (4) kurangnya pelatihan atau pembekalan terkait manajemen risiko keamanan data bagi karyawan. Penelitian ini penting dilakukan untuk mengetahui seberapa efektif manajemen risiko SDM yang diterapkan oleh perusahaan tersebut dalam menghadapi ancaman keamanan data yang terus meningkat. Selain itu, penelitian ini juga diharapkan dapat mengidentifikasi aspek-aspek yang perlu diperkuat dalam kebijakan keamanan data karyawan.

Beberapa penelitian sebelumnya menunjukkan bahwa perusahaan yang mengimplementasikan manajemen risiko SDM dengan baik mampu menekan risiko keamanan data karyawan secara signifikan. Misalnya, penelitian oleh Safitri et al. (2021) menunjukkan bahwa peningkatan protokol keamanan data SDM dapat mengurangi risiko kebocoran data hingga 30%. Sementara itu, Yuliani dan Gunawan (2018) menyatakan bahwa pelatihan keamanan data bagi karyawan memiliki dampak positif dalam meningkatkan kesadaran dan kepatuhan terhadap kebijakan keamanan data. Pemerintah Indonesia sendiri telah mengeluarkan kebijakan yang relevan, seperti Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE), yang menekankan pentingnya perlindungan data pribadi dalam operasional perusahaan. Kebijakan ini menjadi dasar kuat bagi perusahaan untuk memperkuat sistem manajemen risiko yang melibatkan data pribadi, termasuk data karyawan, demi mencegah penyalahgunaan dan kebocoran informasi.

Penelitian ini bertujuan untuk menganalisis efektivitas manajemen risiko sumber daya manusia dalam menangani risiko keamanan data karyawan di perusahaan teknologi, serta memberikan rekomendasi yang relevan untuk meningkatkan perlindungan data tersebut. Penelitian ini diharapkan dapat memberikan gambaran mendalam tentang langkah-langkah yang perlu diambil oleh perusahaan teknologi dalam mengelola risiko data karyawan, serta dapat menjadi acuan bagi pengembangan kebijakan internal perusahaan yang lebih tangguh dalam menghadapi tantangan keamanan data di masa depan.

2. LITERATURE REVIEW

a. Manajemen Risiko Sumber Daya Manusia

Manajemen risiko sumber daya manusia (SDM) adalah pendekatan yang sistematis dalam mengidentifikasi, menganalisis, dan merespon risiko yang berhubungan dengan aspek SDM dalam organisasi. Menurut Drazin dan Van de Ven (2019), manajemen risiko SDM mencakup perencanaan strategis untuk melindungi aset manusia, yang sangat penting dalam menghadapi risiko yang berkaitan dengan keamanan informasi dan data pribadi karyawan. Proses ini melibatkan evaluasi risiko, pembuatan kebijakan yang relevan, dan implementasi prosedur yang dapat meminimalisir potensi risiko.

Manajemen risiko SDM sangat penting bagi organisasi, terutama dalam menghadapi dinamika pasar dan perubahan teknologi yang cepat. Penerapan manajemen risiko yang baik dapat membantu organisasi untuk meminimalisir dampak negatif dari potensi risiko, meningkatkan efisiensi operasional, dan menjaga keberlanjutan bisnis. Menurut Ibrahim et al. (2019), perusahaan yang memiliki sistem manajemen risiko SDM yang efektif mampu beradaptasi lebih baik terhadap perubahan lingkungan bisnis dan mempertahankan daya saing.

Komponen utama dalam manajemen risiko SDM mencakup identifikasi risiko, analisis risiko, perencanaan respon risiko, implementasi, dan pemantauan. Identifikasi risiko melibatkan penilaian terhadap faktor-faktor yang dapat mempengaruhi karyawan, seperti ketidakpuasan kerja, turnover, serta risiko kesehatan dan keselamatan. Setelah risiko diidentifikasi, langkah berikutnya adalah melakukan analisis untuk menentukan dampak dan kemungkinan terjadinya risiko tersebut. Perencanaan respon risiko meliputi strategi untuk mengurangi atau menghindari risiko yang telah diidentifikasi. Menurut D'Amato et al. (2021), pemantauan berkelanjutan terhadap risiko dan efektivitas respon sangat penting untuk memastikan bahwa strategi yang diterapkan tetap relevan dan efektif.

Manajemen Risiko Sumber Daya Manusia merupakan komponen penting dalam menjaga keberlanjutan dan kesuksesan organisasi. Dengan memahami konsep dan pentingnya manajemen risiko ini, organisasi dapat mengidentifikasi dan mengurangi risiko yang dapat mempengaruhi kinerja dan keamanan data karyawan. Penerapan strategi yang efektif, keterlibatan karyawan, serta pemantauan berkelanjutan adalah langkah-langkah krusial untuk mencapai tujuan ini.

b. Keamanan Data Karyawan

Keamanan data karyawan merujuk pada langkah-langkah dan kebijakan yang diterapkan oleh organisasi untuk melindungi informasi pribadi dan sensitif terkait karyawan dari ancaman seperti pencurian identitas, kebocoran data, dan akses tidak sah. Menurut Tso et al. (2021), keamanan data karyawan mencakup perlindungan terhadap informasi seperti nomor identitas, informasi rekening bank, dan riwayat pekerjaan yang jika jatuh ke tangan yang salah dapat merugikan karyawan dan organisasi. Keamanan data merupakan komponen penting dalam manajemen risiko dan bertujuan untuk menciptakan kepercayaan antara karyawan dan perusahaan.

Keamanan data karyawan sangat penting, terutama dalam era digital di mana informasi lebih rentan terhadap serangan siber. Kebocoran data dapat menyebabkan kerugian finansial yang signifikan, merusak reputasi perusahaan, dan mengurangi kepercayaan karyawan. Menurut Kshetri (2017), organisasi yang gagal melindungi data karyawan berisiko menghadapi sanksi hukum dan kerugian reputasi yang dapat mempengaruhi operasional jangka panjang. Oleh karena itu, investasi dalam sistem keamanan data yang efektif menjadi krusial untuk menjaga integritas dan kerahasiaan informasi.

Berbagai risiko dapat mengancam keamanan data karyawan, termasuk serangan siber, kebocoran informasi internal, dan penggunaan perangkat yang tidak aman. Serangan siber seperti phishing, malware, dan ransomware merupakan ancaman serius yang dapat mengakibatkan pencurian data karyawan. Menurut Warkentin et al. (2019), tingginya tingkat penggunaan perangkat pribadi (BYOD) di tempat kerja juga meningkatkan risiko kebocoran data, karena perangkat ini sering kali tidak dilengkapi dengan keamanan yang memadai. Oleh karena itu, penting bagi organisasi untuk memahami dan mengelola risiko-risiko ini secara proaktif.

c. Strategi Manajemen Risiko dalam Keamanan Data

Manajemen risiko keamanan data adalah proses yang sistematis untuk mengidentifikasi, mengevaluasi, dan mengelola risiko yang berkaitan dengan keamanan informasi dalam organisasi. Strategi ini bertujuan untuk melindungi data sensitif dari ancaman internal dan eksternal, serta memastikan bahwa organisasi dapat beroperasi dengan aman dan efektif. Menurut ISO 27001, standar internasional untuk manajemen keamanan informasi, pendekatan berbasis risiko dalam manajemen keamanan data memungkinkan organisasi untuk fokus pada area yang paling rentan dan memprioritaskan sumber daya untuk melindungi informasi yang paling kritis (ISO, 2018).

Strategi manajemen risiko keamanan data biasanya melibatkan beberapa langkah kunci, termasuk:

i. Identifikasi Risiko: Menentukan jenis risiko yang dapat mempengaruhi keamanan data, seperti serangan siber, kesalahan manusia, dan bencana alam.
ii. Analisis Risiko: Mengkaji kemungkinan dan dampak dari risiko yang telah diidentifikasi untuk menentukan prioritas.
iii. Perencanaan Respon Risiko: Mengembangkan rencana untuk mengatasi risiko yang telah dianalisis, termasuk mitigasi, transfer, atau penerimaan risiko.
iv. Implementasi dan Monitoring: Melaksanakan rencana yang telah dikembangkan dan memantau efektivitasnya secara berkala untuk memastikan bahwa strategi tetap relevan dengan perkembangan ancaman yang ada (Bishop & Gates, 2019).

3. METODE

Penelitian ini menggunakan pendekatan kualitatif yang bertujuan untuk memahami fenomena yang berkaitan dengan efektivitas manajemen risiko sumber daya manusia dalam menghadapi risiko keamanan data karyawan. Pendekatan ini memungkinkan peneliti untuk menggali pengalaman, pandangan, dan persepsi yang mendalam dari responden terkait dengan kebijakan dan praktik manajemen risiko yang diterapkan di perusahaan teknologi.

4. HASIL & DISKUSI

Hasil (Temuan)

Hasil analisis literatur sistematis menunjukkan bahwa terdapat sejumlah faktor yang mempengaruhi efektivitas manajemen risiko sumber daya manusia dalam menghadapi risiko keamanan data. Dari 20 artikel yang dianalisis, ditemukan bahwa keberadaan kebijakan dan prosedur keamanan yang jelas sangat penting untuk mengarahkan tindakan karyawan dalam melindungi data. Sebagian besar studi menunjukkan bahwa kebijakan ini harus dikomunikasikan dengan baik kepada semua karyawan (Gu et al., 2022; Arachchilage & Love, 2014). Selain itu, pelatihan karyawan juga merupakan faktor kunci, di mana perusahaan yang memberikan pelatihan keamanan data yang rutin kepada karyawan memiliki tingkat kepatuhan yang lebih tinggi terhadap kebijakan keamanan.

Penelitian oleh Böhme (2015) menegaskan bahwa pelatihan meningkatkan kesadaran dan kemampuan karyawan dalam mengelola risiko. Hasil analisis juga menunjukkan bahwa penggunaan teknologi, seperti firewall, enkripsi, dan software deteksi intrusi, berperan

penting dalam mendukung kebijakan manajemen risiko, dengan penelitian Khan dan Alghamdi (2020) yang menunjukkan bahwa investasi dalam sistem keamanan terbukti efektif dalam mengurangi risiko pelanggaran data. Selain itu, budaya organisasi yang mendukung keamanan informasi, termasuk dukungan manajemen puncak, juga berkontribusi terhadap efektivitas manajemen risiko, seperti yang diungkapkan oleh Siponen et al. (2016). Proses evaluasi dan pengumpulan umpan balik dari karyawan juga ditemukan penting untuk meningkatkan kebijakan manajemen risiko, yang membantu penyesuaian kebijakan agar sesuai dengan kebutuhan dan tantangan yang dihadapi (Weber et al., 2019). Secara keseluruhan, efektivitas manajemen risiko sumber daya manusia dalam menghadapi risiko keamanan data dipengaruhi oleh kombinasi dari kebijakan yang jelas, pelatihan yang memadai, penggunaan teknologi yang tepat, budaya organisasi yang mendukung, serta proses evaluasi yang berkelanjutan.

Pembahasan

Pembahasan mengenai hasil penelitian ini menunjukkan bahwa kebijakan dan prosedur keamanan yang jelas serta terstruktur menjadi dasar penting dalam manajemen risiko. Menurut Gu et al. (2022), keberadaan kebijakan yang dirumuskan dengan baik memberikan arahan bagi karyawan dalam melaksanakan tugas mereka dengan memperhatikan keamanan data. Hal ini sejalan dengan penelitian sebelumnya yang menekankan bahwa komunikasi yang efektif mengenai kebijakan tersebut akan meningkatkan kesadaran dan pemahaman karyawan (Arachchilage & Love, 2014).

Selain itu, pelatihan karyawan terkait keamanan data merupakan faktor kunci dalam meningkatkan efektivitas manajemen risiko. Böhme (2015) menyoroti bahwa perusahaan yang rutin memberikan pelatihan keamanan data tidak hanya meningkatkan kesadaran karyawan tetapi juga memperkuat kompetensi mereka dalam menangani potensi risiko. Oleh karena itu, perusahaan perlu menginvestasikan waktu dan sumber daya untuk menyusun program pelatihan yang efektif. Penggunaan teknologi juga berperan penting dalam mendukung manajemen risiko.

Menurut Khan dan Alghamdi (2020), investasi dalam sistem keamanan informasi yang canggih dapat mengurangi risiko pelanggaran data secara signifikan. Teknologi seperti enkripsi, firewall, dan software deteksi intrusi tidak hanya melindungi data, tetapi juga memberikan kepercayaan lebih bagi karyawan dalam mengelola informasi sensitif.

Selanjutnya, budaya organisasi yang mendukung keamanan informasi juga sangatberpengaruh. Siponen et al. (2016) menunjukkan bahwa dukungan dari manajemen puncak terhadap kebijakan keamanan dapat menciptakan lingkungan kerja yang aman.

Organisasi yang mendorong keterlibatan dan partisipasi karyawan dalam aspek keamanan cenderung lebih sukses dalam mengimplementasikan praktik manajemen risiko. Terakhir, proses evaluasi yang berkelanjutan serta pengumpulan umpan balik dari karyawan merupakan bagian penting dalam manajemen risiko. Weber et al. (2019) mencatat bahwa organisasi yang secara aktif melakukan evaluasi dan memperbaiki kebijakan mereka berdasarkan umpan balik dapat lebih adaptif terhadap perubahan dan tantangan baru dalam keamanan data. Oleh karena itu, perusahaan harus mengembangkan mekanisme untuk mendengarkan suara karyawan dan menyesuaikan kebijakan keamanan sesuai kebutuhan.

5. KESIMPULAN

Penelitian tentang efektivitas manajemen risiko sumber daya manusia dalam menghadapi risiko keamanan data karyawan di sektor teknologi menunjukkan bahwa terdapat beberapa faktor kunci yang mempengaruhi keberhasilan dalam melindungi data karyawan. Kebijakan dan prosedur keamanan yang jelas sangat penting sebagai pedoman bagi karyawan dalam melaksanakan tugas mereka dengan memperhatikan keamanan data. Pelatihan yang rutin dan efektif terbukti meningkatkan kesadaran dan kompetensi karyawan dalam menghadapi potensi risiko, sehingga perusahaan perlu mengalokasikan sumber daya yang memadai untuk program pelatihan tersebut.

Penggunaan teknologi yang tepat, seperti enkripsi dan sistem deteksi intrusi, berperan signifikan dalam mendukung kebijakan keamanan dan mengurangi risiko pelanggaran data. Selain itu, budaya organisasi yang mendukung keamanan informasi, ditandai dengan dukungan dari manajemen puncak, menciptakan lingkungan yang kondusif bagi penerapan praktik manajemen risiko yang efektif. Terakhir, proses evaluasi yang berkelanjutan dan pengumpulan umpan balik dari karyawan merupakan langkah penting dalam memastikan bahwa kebijakan keamanan tetap relevan dan adaptif terhadap perkembangan tantangan keamanan yang ada.

Dengan demikian, untuk meningkatkan efektivitas manajemen risiko sumber daya manusia dalam menghadapi risiko keamanan data karyawan, perusahaan di sektor teknologi harus mengintegrasikan kebijakan yang jelas, program pelatihan yang efektif, penerapan teknologi yang canggih, serta membangun budaya organisasi yang mendukung keamanan informasi. Langkah-langkah ini tidak hanya akan melindungi data karyawan tetapi juga meningkatkan kepercayaan dan keterlibatan karyawan dalam upaya keamanan data di perusahaan.

REFERENCES

Arachchilage, N. A. G., & Love, S. (2014). The role of employee awareness in information security: A study of the role of training. Computers & Security, 43, 265-273.

Bishop, P., & Gates, S. (2019). Managing cybersecurity risk: The importance of risk assessments. Journal of Cybersecurity Technology, 3(2), 98-113.

Böhme, R. (2015). Security and privacy in the digital age. IEEE Security & Privacy, 13(2), 7-11.

D'Amato, A., D'Ambrosio, A., & Sorrentino, A. (2021). Human resource risk management: Theoretical perspectives and future directions. Human Resource Management, 60(3), 421-436.

Drazin, R., & Van de Ven, A. H. (2019). Toward a theory of organization as a human system. Academy of Management Review, 44(3), 123-139.

Gu, Y., Zhu, S., & Li, X. (2022). The role of organizational culture in security policy compliance: A study of information security management. Journal of Business Research, 142, 96-107.

Hasanah, R., & Priatna, R. (2017). Analisis implementasi manajemen risiko sumber daya manusia untuk keamanan informasi di sektor teknologi. Jurnal Pengelolaan Teknologi dan Informasi, 10(3), 91-104.

Hayton, J. C., & Kelley, D. (2014). Managing human resource risk in organizations: A conceptual framework. International Journal of Human Resource Management, 25(9), 1254-1270.

Ibrahim, A., Nader, A., & Zulkifli, A. (2019). The impact of human resource risk management on organizational performance. International Journal of Management, 10(4), 227-238.

International Organization for Standardization (ISO). (2018). ISO/IEC 27001:2018 - Information security management systems. Geneva: ISO.

Jatmiko, A., Fitriani, F., & Rahman, A. (2022). Proactive risk management strategies for data security in the digital workplace. Jurnal Sistem Informasi dan Teknologi, 14(2), 100-113.

Khan, M. A., & Alghamdi, R. (2020). Impact of information technology on data security management: A study of banking sector. Journal of Information Security and Applications, 54, 102557.

Kshetri, N. (2017). Cybersecurity and data privacy: A growing concern for businesses. In The Cybersecurity and Privacy Handbook (pp. 1-19).

Pemerintah Indonesia. (2019). Peraturan Pemerintah No. 71 Tahun 2019: Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE). Jakarta: Pemerintah Indonesia.

Safitri, L., & Kurniawati, A. (2021). Pengaruh manajemen risiko sumber daya manusia terhadap keamanan data karyawan di perusahaan teknologi. Jurnal Teknologi dan Keamanan Data, 15(2), 134-146.

Sharma, R., & Gupta, N. (2020). Enhancing data security awareness among employees: A study on the role of training. International Journal of Information Management, 50, 1-10.

Siponen, M., Kannan, G., & Li, X. (2016). Information security compliance: An integration of the human factor and the technology factor. Computers & Security, 58, 52-66.

Sutrisno, A., & Kurnia, D. (2019). Evaluasi sistem keamanan data karyawan dalam perspektif manajemen risiko SDM. Jurnal Pengembangan Teknologi Informasi, 13(4), 213-227.

Tso, K. C., Liang, C. S., & Wu, J. (2021). Data protection and privacy management: A new perspective in the workplace. International Journal of Information Management, 56, 102-112.

Warkentin, M., et al. (2019). Cybersecurity and employee behavior: A behavioral perspective. Computers & Security, 86, 189-203.

Weber, R. H., et al. (2019). Information security management: The influence of risk assessment, compliance, and information technology. Journal of Information Systems and Technology Management, 16(2), 15-31.

Yuliani, M., & Gunawan, A. (2018). Pentingnya pelatihan keamanan data dalam mengurangi risiko kebocoran informasi di perusahaan teknologi. Jurnal Manajemen Teknologi Indonesia, 12(1), 67-80.