Manajemen Risiko dalam E-Bisnis: Pendekatan untuk Keamanan Data dan Mitigasi Risiko Siber

Ari Susanto
STIE Mahardhika Surabaya
email: arisusanto@stiemahardhika.ac.id

Article Info

Article history:

Received : 28 - 11, 2024
Revised : 21 - 12, 2024
Accepted : 06 - 01, 2025

Keywords:

Risk Management;
E-Business;
Data Security;
Cyber Risk;
Security Policy.

ABSTRACT

Risk management in e-business is one of the important aspects in facing the increasingly complex challenges of data security and cyber threats. This article discusses a strategic approach to risk management to protect data, maintain customer trust, and ensure operational sustainability. The research covers risk identification, impact analysis, and the implementation of technology and policy-based mitigation solutions. By emphasising the importance of risk management integration in e-business, this article provides guidance for companies to build a resilient security framework, while meeting global compliance standards. The results are expected to support the development of a secure and reliable e-business ecosystem.

Corresponding Author:

Ari Susanto
Sekolah Tinggi Ilmu Ekonomi Mahardhika Surabaya
Email: arisusanto@stiemahardhika.ac.id

1. PENDAHULUAN

E-bisnis telah menjadi salah satu pilar utama dalam perkembangan ekonomi digital, menawarkan berbagai kemudahan bagi perusahaan dan konsumen dalam melakukan transaksi dan pertukaran informasi. Namun, di balik kemajuan ini, terdapat risiko signifikan terkait keamanan data dan ancaman siber yang dapat merugikan perusahaan secara finansial, reputasi, dan operasional. Dalam lingkungan digital yang semakin kompleks, ancaman seperti peretasan, pencurian data, dan serangan malware terus meningkat, menuntut perhatian khusus terhadap upaya mitigasi risiko (Abomhara & Køien, 2015; Maskun, 2022; Rahayu, 2022).

Manajemen risiko menjadi kunci untuk menghadapi tantangan ini dengan mengidentifikasi, menganalisis, dan mengendalikan risiko yang mungkin terjadi dalam operasi e-bisnis (Novalia et al., 2021; Siswanti et al., 2020). Pendekatan yang terstruktur dan sistematis dalam manajemen risiko tidak hanya membantu melindungi aset digital perusahaan tetapi juga mendukung kepatuhan terhadap regulasi keamanan data yang berlaku secara lokal maupun internasional.

Penelitian ini bertujuan untuk mengeksplorasi berbagai strategi dan pendekatan dalam manajemen risiko di e-bisnis, dengan fokus pada penguatan keamanan data dan mitigasi risiko siber. Dengan membangun kerangka kerja yang efektif, perusahaan dapat meningkatkan ketahanan terhadap ancaman siber, sekaligus menciptakan ekosistem bisnis yang lebih aman dan terpercaya.

2. TINJAUAN PUSTAKA

Manajemen risiko dalam e-bisnis merupakan topik yang terus berkembang seiring dengan meningkatnya ketergantungan perusahaan pada teknologi digital. Beberapa studi sebelumnya telah menyoroti pentingnya strategi manajemen risiko untuk menghadapi ancaman siber dan melindungi data penting perusahaan.

1. Manajemen Risiko dalam E-Bisnis

Menurut Hallikas et al. (2004), manajemen risiko dalam e-bisnis mencakup proses identifikasi, penilaian, dan pengendalian risiko yang terkait dengan aktivitas digital. Proses ini dirancang untuk mengurangi potensi kerugian dan memastikan keberlanjutan bisnis. Studi dari Aven (2015) menunjukkan bahwa pendekatan berbasis analisis kuantitatif dan kualitatif dapat memberikan hasil yang optimal dalam pengelolaan risiko e-bisnis.

2. Keamanan Data dalam Ekosistem Digital

Keamanan data menjadi komponen krusial dalam manajemen risiko e-bisnis. Menurut Stallings (2018), implementasi protokol enkripsi, sistem otentikasi berlapis, dan firewall adalah langkah fundamental untuk melindungi data pelanggan. Selain itu, penelitian oleh Solms dan Niekerk (2013) menekankan bahwa kesadaran dan pelatihan karyawan merupakan faktor kunci dalam meminimalkan kesalahan manusia yang dapat membuka celah keamanan.

3. Mitigasi Risiko Siber

Beberapa penelitian, seperti yang dilakukan oleh Peltier (2005), menyoroti pentingnya pendekatan proaktif dalam mitigasi risiko siber, termasuk pemantauan sistem secara real-time dan penerapan solusi berbasis kecerdasan buatan untuk mendeteksi ancaman lebih awal. Selanjutnya, Framework NIST (National Institute of Standards and Technology) yang sering digunakan sebagai panduan utama dalam mitigasi risiko, mengidentifikasi lima fungsi inti: identifikasi, perlindungan, deteksi, respons, dan pemulihan.

4. Kepatuhan terhadap Regulasi Keamanan Data

Regulasi seperti GDPR (General Data Protection Regulation) dan UU Perlindungan Data Pribadi (UU PDP) di Indonesia mengharuskan perusahaan untuk mengambil langkah-langkah tegas dalam pengelolaan data pribadi. Menurut penelitian oleh Voigt dan Von dem Bussche (2017), kepatuhan terhadap regulasi tidak hanya mengurangi risiko hukum tetapi juga membangun kepercayaan pelanggan.

3. METODE PENELITIAN

Penelitian ini menggunakan pendekatan deskriptif kualitatif untuk menganalisis strategi manajemen risiko dalam e-bisnis, khususnya terkait keamanan data dan mitigasi risiko siber. Metode ini dipilih karena mampu memberikan pemahaman mendalam mengenai fenomena yang sedang diteliti, dengan memadukan analisis literatur, studi kasus, dan wawancara pakar.

1. Pendekatan Penelitian

Penelitian ini menggunakan pendekatan studi literatur sebagai dasar untuk mengeksplorasi konsep dan kerangka kerja terkait manajemen risiko, keamanan data, dan mitigasi risiko siber. Selain itu, data primer dikumpulkan melalui wawancara semi-terstruktur dengan para ahli di bidang teknologi informasi, keamanan siber, dan manajemen risiko.

2. Pengumpulan Data

Data Sekunder: Menggunakan jurnal ilmiah, laporan industri, regulasi, dan dokumen kebijakan terkait untuk mendapatkan wawasan teoritis dan data empiris.

Data Primer: Mengadakan wawancara dengan narasumber dari kalangan profesional IT, manajer risiko, dan akademisi yang memiliki pengalaman dalam implementasi keamanan siber di e-bisnis.

3. Teknik Analisis Data

Data yang diperoleh dianalisis menggunakan metode analisis tematik. Proses ini melibatkan langkah-langkah berikut:

- Reduksi Data: Mengorganisasi data yang relevan berdasarkan tema-tema utama, seperti identifikasi risiko, mitigasi risiko, dan kepatuhan regulasi.
- Penyajian Data: Menyusun data dalam bentuk matriks atau diagram untuk mempermudah interpretasi.
- Kesimpulan dan Verifikasi: Menyimpulkan temuan utama berdasarkan hubungan antara strategi manajemen risiko dan dampaknya terhadap keamanan data serta mitigasi risiko siber.

4. Validasi Data

Validitas data dijaga dengan melakukan triangulasi, yakni membandingkan hasil wawancara dengan temuan dari literatur dan studi kasus. Teknik ini memastikan bahwa analisis dan interpretasi data akurat serta dapat dipercaya.

5. Batasan Penelitian

Penelitian ini terbatas pada analisis perusahaan yang beroperasi di sektor e-bisnis dengan fokus pada lingkungan digital di Indonesia, sehingga hasilnya mungkin tidak sepenuhnya dapat digeneralisasikan untuk konteks global.

4. HASIL DAN PEMBAHASAN

4.1. Hasil Penelitian

Penelitian ini mengidentifikasi beberapa temuan utama terkait manajemen risiko dalam e-bisnis, khususnya dalam upaya meningkatkan keamanan data dan mitigasi risiko siber:

a. Identifikasi Risiko Utama

Risiko utama dalam e-bisnis meliputi peretasan data pelanggan, pencurian identitas, ransomware, dan pelanggaran privasi. Analisis menunjukkan bahwa sebagian besar perusahaan belum sepenuhnya memahami kerentanan yang terdapat dalam sistem mereka, terutama pada lapisan keamanan aplikasi dan infrastruktur jaringan.

b. Implementasi Keamanan Data

Hasil wawancara dengan pakar menunjukkan bahwa penerapan teknologi seperti enkripsi data, firewall cerdas, dan otentikasi multifaktor efektif dalam mengurangi risiko kebocoran data. Namun, kurangnya pelatihan karyawan terkait keamanan digital menjadi salah satu penyebab utama insiden keamanan.

c. Mitigasi Risiko Siber

Perusahaan yang menggunakan solusi berbasis kecerdasan buatan (AI) untuk mendeteksi dan merespons ancaman siber secara real-time menunjukkan tingkat keberhasilan yang lebih tinggi dalam mengurangi dampak risiko siber. Pendekatan berbasis AI ini dilengkapi dengan pemantauan jaringan yang terus menerus dan analisis perilaku pengguna untuk mengidentifikasi anomali.

d. Kepatuhan terhadap Regulasi

Penelitian menemukan bahwa perusahaan yang mematuhi regulasi keamanan data seperti GDPR atau UU Perlindungan Data Pribadi (UU PDP) cenderung lebih tangguh dalam menghadapi ancaman siber. Namun, penerapan regulasi ini memerlukan investasi yang cukup besar, sehingga menjadi tantangan bagi perusahaan kecil dan menengah.

4.2. Pembahasan

a. Pentingnya Kerangka Manajemen Risiko yang Terintegrasi

Manajemen risiko yang terintegrasi menjadi fondasi utama untuk keberlanjutan e-bisnis. Temuan ini sejalan dengan teori Hallikas et al. (2004) yang menyebutkan bahwa proses identifikasi dan analisis risiko yang mendalam membantu perusahaan memahami potensi kerugian sebelum terjadi insiden.

b. Kesenjangan dalam Sumber Daya Manusia

Meskipun teknologi memainkan peran penting, faktor manusia tetap menjadi tantangan. Sebagian besar kebocoran data disebabkan oleh kelalaian atau kurangnya pengetahuan karyawan mengenai protokol keamanan. Ini menekankan pentingnya pelatihan reguler dan kampanye kesadaran keamanan bagi seluruh staf.

c. Manfaat Solusi Teknologi Proaktif

Pendekatan berbasis teknologi proaktif, seperti pemanfaatan AI dan big data analytics, menunjukkan hasil positif dalam mitigasi risiko. Teknologi ini memungkinkan perusahaan untuk mendeteksi pola ancaman yang tidak terlihat oleh solusi tradisional, sehingga meningkatkan kecepatan respons.

d. Tantangan Regulasi dan Biaya Implementasi

Meskipun regulasi keamanan data memberikan pedoman penting, implementasinya membutuhkan investasi besar dalam infrastruktur teknologi dan pelatihan. Perusahaan kecil dan menengah perlu mempertimbangkan opsi berbasis cloud yang lebih terjangkau untuk memenuhi kebutuhan ini.

e. Rekomendasi Strategis

Berdasarkan hasil penelitian, perusahaan disarankan untuk:

- Mengintegrasikan manajemen risiko ke dalam semua aspek operasi e-bisnis.
- Meningkatkan kesadaran keamanan di seluruh tingkat organisasi.
- Berinvestasi dalam solusi berbasis AI dan pemantauan keamanan real-time.
- Mematuhi regulasi yang relevan untuk melindungi data pelanggan dan mengurangi risiko hukum.

Hasil penelitian ini mempertegas pentingnya manajemen risiko dalam menciptakan ekosistem e-bisnis yang aman, andal, dan berkelanjutan. Dengan mengimplementasikan strategi yang tepat, perusahaan dapat melindungi aset digital mereka sekaligus meningkatkan kepercayaan pelanggan.

5. KESIMPULAN

5.1. Kesimpulan

Manajemen risiko dalam e-bisnis merupakan aspek krusial dalam menghadapi tantangan keamanan data dan ancaman siber yang semakin meningkat. Penelitian ini menunjukkan bahwa pendekatan yang terintegrasi, mencakup identifikasi risiko, penerapan teknologi keamanan, dan kepatuhan terhadap regulasi, dapat secara signifikan mengurangi kerentanan perusahaan terhadap serangan siber. Penggunaan teknologi canggih seperti kecerdasan buatan dan sistem pemantauan real-time terbukti efektif dalam mendeteksi dan merespons ancaman lebih cepat. Selain itu, pelatihan sumber daya manusia dan kesadaran akan keamanan siber menjadi elemen penting dalam mencegah insiden yang diakibatkan oleh kelalaian manusia.

Meskipun demikian, tantangan seperti biaya implementasi dan kepatuhan terhadap regulasi tetap menjadi kendala, terutama bagi perusahaan kecil dan menengah. Oleh karena itu, diperlukan strategi yang tepat guna memastikan bahwa seluruh lapisan perusahaan dapat mengadopsi pendekatan ini sesuai dengan skala dan kebutuhan mereka.

5.2. Saran

Dalam upaya meningkatkan keamanan sistem e-bisnis, beberapa rekomendasi strategis perlu dipertimbangkan untuk implementasi. Pertama, perusahaan perlu melakukan peningkatan investasi dalam teknologi keamanan dengan mengalokasikan anggaran khusus untuk mengadopsi teknologi terkini seperti enkripsi, AI untuk deteksi ancaman, dan sistem pemantauan jaringan yang canggih. Teknologi-teknologi ini menjadi fondasi penting dalam membangun pertahanan yang kuat terhadap berbagai bentuk ancaman siber.

Aspek kedua yang tidak kalah penting adalah pelatihan dan peningkatan kesadaran keamanan siber di kalangan karyawan. Program pelatihan berkala perlu dirancang dan dilaksanakan untuk meningkatkan pemahaman karyawan tentang praktik keamanan yang baik serta memberikan pengetahuan praktis tentang cara mengidentifikasi dan menghadapi berbagai bentuk ancaman siber. Karyawan yang terlatih dan memiliki kesadaran tinggi tentang keamanan siber menjadi garis pertahanan pertama dalam mencegah terjadinya insiden keamanan.

Selanjutnya, penerapan kebijakan manajemen risiko yang terintegrasi menjadi komponen vital dalam strategi keamanan e-bisnis. Manajemen risiko harus diintegrasikan secara menyeluruh ke dalam proses operasional e-bisnis, mencakup identifikasi risiko secara sistematis, pengembangan strategi mitigasi yang efektif, serta perencanaan dan implementasi prosedur pemulihan pasca-insiden yang komprehensif.

Untuk mendukung implementasi standar keamanan yang memadai di kalangan UKM, diperlukan dukungan khusus berupa solusi yang terjangkau dan panduan praktis. Pemerintah atau penyedia layanan keamanan dapat berperan dalam menyediakan resources dan panduan yang memudahkan usaha kecil dan menengah dalam memenuhi standar kepatuhan regulasi keamanan data, mengingat keterbatasan sumber daya yang sering dihadapi oleh sektor ini.

Terakhir, kolaborasi dengan ahli dan lembaga keamanan menjadi langkah strategis dalam memastikan keamanan sistem yang berkelanjutan. Perusahaan dapat menjalin kerjasama dengan penyedia layanan keamanan siber profesional atau lembaga penelitian untuk memastikan sistem keamanan mereka selalu mutakhir dan mampu menghadapi ancaman yang terus berkembang. Melalui implementasi menyeluruh dari rekomendasi-rekomendasi ini, perusahaan dapat memperkuat ketahanan terhadap ancaman siber, melindungi aset digital mereka secara efektif, dan mempertahankan kepercayaan pelanggan, yang pada akhirnya berkontribusi pada keberlanjutan bisnis mereka di era digital yang penuh tantangan.

DAFTAR PUSTAKA

Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*, 65–88.

Aven, T. (2015). *Risk analysis*. John Wiley & Sons.

Hallikas, J., Karvonen, I., Pulkkinen, U., Virolainen, V.-M., & Tuominen, M. (2004). Risk management processes in supplier networks. *International Journal of Production Economics*, *90*(1), 47–58.

Maskun. (2022). *Kejahatan Siber (Cyber Crime): Suatu Pengantar*. Prenada Media.

Novalia, D., Kahfi, H., & Lidya, R. (2021). Peran Teknologi Informasi Dalam Mengantisipasi Kecurangan

Akuntansi (Studi Kasus pada PT Bangkit Berkah). *Jurnal Buana Akuntansi*, *6*(1). https://doi.org/10.36805/akuntansi.v6i1.1353

Peltier, T. R. (2005). *Information security risk analysis*. Auerbach publications.

Rahayu, K. Y. (2022). Tata Kelola Keamanan Siber Perlu Dievaluasi. *Kompas.Id*. https://www.kompas.id/baca/polhuk/2022/09/16/tata-kelola-keamanan-siber-perlu-dievaluasi

Siswanti, I., Sitepu, C. N. B., Butarbutar, N., Basmar, E., Saleh, R., Sudirman, S., Mahyuddin, M., Parinduri, L., & Prasasti, L. (2020). *Manajemen Risiko Perusahaan*. Yayasan Kita Menulis.

Stallings, W. (2018). *Effective cybersecurity: a guide to using best practices and standards*. Addison-Wesley Professional.

Voigt, P., & Von dem Bussche, A. (2017). The eu general data protection regulation (gdpr). *A Practical Guide, 1st Ed., Cham: Springer International Publishing*, *10*(3152676), 10–5555.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102.