Jurnal Visi Manajemen
Volume 10 Nomor 3 Tahun 2024
E-ISSN: 2528-2212 P-ISSN: 2303-3339, Hal 283-296
DOI: https://doi.org/10.56910/jvm.v10i3.586
Available online at: https://stiepari.org/index.php/jvm

Pengungkapan Risiko Keamanan Siber: Dampaknya Terhadap Hubungan Pelanggan-Pemasok Dalam Rantai Pasok Perusahaan

Mohammad Chaidir[1], Ngadi Permana[2], Grace Yulianti[3]
[1,2,3] STIE Kasih Bangsa, Indonesia
Email : m.chaidir@stiekasihbangsa.ac.id [1], ngadi.permana@stiekasihbangsa.ac.id [2], grace@stiekasihbangsa.ac.id [3]

Abstract. *This study explores the impact of cybersecurity risk disclosure on customer-supplier relationships in corporate supply chains through a qualitative literature review approach. The findings reveal that transparency in cybersecurity risk disclosure enhances trust, relationship stability, and operational efficiency within supply chains. Conversely, a lack of disclosure or poor risk management can damage reputations, create uncertainty, and weaken collaboration between business partners. The study also highlights the importance of adequate regulations, risk mitigation strategies, and the adoption of new technologies in managing cybersecurity. While offering significant insights, this study has limitations, including reliance on secondary literature and variations in industry contexts. Future research is recommended to include empirical testing and the exploration of new technologies to strengthen cybersecurity risk management in supply chains.*

Keywords: *Customer-Supplier Relationships, Cybersecurity Risk Disclosure, Cybersecurity, Information Transparency, Supply Chains*

Abstrak. Penelitian ini mengeksplorasi dampak pengungkapan risiko keamanan siber terhadap hubungan pelanggan-pemasok dalam rantai pasok perusahaan melalui pendekatan kualitatif literatur review. Hasil penelitian menunjukkan bahwa transparansi dalam pengungkapan risiko siber dapat meningkatkan kepercayaan, stabilitas hubungan, dan efisiensi operasional dalam rantai pasok. Sebaliknya, kurangnya pengungkapan atau pengelolaan risiko yang buruk dapat merusak reputasi, menciptakan ketidakpastian, dan melemahkan kolaborasi antar mitra bisnis. Penelitian ini juga mengidentifikasi pentingnya regulasi yang memadai, strategi mitigasi risiko, dan adopsi teknologi baru dalam pengelolaan keamanan siber. Meskipun memberikan wawasan yang signifikan, penelitian ini memiliki keterbatasan, termasuk ketergantungan pada literatur sekunder dan variasi konteks industri. Rekomendasi penelitian selanjutnya mencakup pengujian empiris dan eksplorasi teknologi baru untuk memperkuat pengelolaan risiko siber dalam rantai pasok.

Keyword: Hubungan Pelanggan-Pemasok, Pengungkapan Risiko Siber, Keamanan Siber, Transparansi Informasi, Rantai Pasok.

PENDAHULUAN

Dalam era digital yang semakin berkembang, peran keamanan siber telah menjadi elemen strategis bagi perusahaan dalam melindungi informasi sensitif dan menjaga kelangsungan operasi bisnis. Transformasi digital yang pesat telah meningkatkan ketergantungan perusahaan pada teknologi informasi dan komunikasi, termasuk dalam manajemen rantai pasok (Gordon et al., 2006; AICPA, 2018). Namun, perkembangan ini juga meningkatkan paparan risiko keamanan siber yang dapat berdampak signifikan pada hubungan pelanggan-pemasok, sebuah dimensi kritis dalam rantai pasok perusahaan (Crosignani et al., 2023). Pengungkapan risiko keamanan siber telah menjadi perhatian utama dalam tata kelola perusahaan, terutama setelah diterbitkannya pedoman oleh Securities and Exchange Commission (SEC) pada tahun 2011

Received: Agustus 20, 2024; Revised: Agustus 30, 2024; Accepted: September 28, 2024; Published: September 30, 2024

yang menekankan pentingnya pelaporan risiko keamanan siber (SEC, 2011). Penelitian menunjukkan bahwa transparansi dalam pengungkapan risiko ini dapat memengaruhi hubungan pelanggan-pemasok, terutama dalam membangun kepercayaan di antara para pemangku kepentingan (Chen et al., 2019; Nelson & Schwartz, 2019).

Penelitian ini bertujuan untuk menganalisis dampak pengungkapan risiko keamanan siber terhadap hubungan pelanggan-pemasok dalam konteks rantai pasok perusahaan. Berdasarkan analisis literatur yang komprehensif, penelitian ini mengungkap bagaimana pengungkapan risiko keamanan siber memengaruhi keputusan pembelian pelanggan dan investasi pemasok, serta bagaimana faktor-faktor seperti kualitas informasi dan sifat hubungan memengaruhi durasi hubungan ini (Amir et al., 2018; Bauer et al., 2018). Keamanan siber menjadi salah satu perhatian utama dalam bisnis modern karena dampaknya yang luas terhadap berbagai aspek operasional dan strategis perusahaan. Sebagai contoh, perusahaan yang gagal mengelola risiko keamanan siber dengan baik dapat mengalami kerugian finansial, reputasi, hingga kehilangan pelanggan (Martin et al., 2017; Hinz et al., 2015). Selain itu, transparansi dalam pengungkapan risiko keamanan siber memainkan peran penting dalam memastikan akuntabilitas perusahaan di mata investor dan mitra bisnis (Haapamäki & Sihvonen, 2019).

Dalam konteks rantai pasok, pelanggan cenderung meningkatkan pembelian dari pemasok yang memiliki skor kesadaran keamanan siber yang tinggi. Hal ini mengindikasikan bahwa keamanan siber tidak hanya menjadi isu teknis tetapi juga faktor strategis dalam hubungan bisnis (Nelson, 2018). Penelitian juga menunjukkan bahwa pengungkapan risiko keamanan siber dapat membantu perusahaan memitigasi dampak negatif dari berita buruk yang tidak dipublikasikan, seperti insiden siber yang belum terungkap secara publik (Ashraf, 2022). Hubungan pelanggan-pemasok memainkan peran penting dalam menentukan keberhasilan rantai pasok perusahaan. Penelitian sebelumnya menunjukkan bahwa konsentrasi basis pelanggan dapat memengaruhi kinerja dan inovasi perusahaan, dengan pelanggan besar seringkali memiliki pengaruh yang signifikan terhadap pemasok mereka (Chen et al., 2022; Irvine et al., 2016). Dalam konteks keamanan siber, pelanggan yang memiliki informasi yang lebih baik tentang risiko pemasok mereka cenderung membuat keputusan yang lebih rasional terkait hubungan bisnis mereka (Chen et al., 2019; Raman & Shahrur, 2008). Ketika pelanggan memiliki akses terhadap informasi risiko keamanan siber pemasok, mereka dapat menilai risiko ini secara lebih akurat dan menyesuaikan keputusan pembelian mereka. Penelitian Crosignani et al. (2023) menemukan bahwa serangan siber dapat menyebar melalui rantai pasok, sehingga meningkatkan pentingnya pengungkapan risiko keamanan siber untuk memitigasi risiko sistemik dalam hubungan pelanggan-pemasok. Pengungkapan risiko keamanan siber memiliki

implikasi yang luas bagi pembuat kebijakan, manajer rantai pasok, dan regulator. SEC, misalnya, telah menetapkan pedoman yang mendorong perusahaan untuk meningkatkan transparansi dalam pengungkapan risiko keamanan siber (SEC, 2011). Selain itu, kerangka pelaporan manajemen risiko keamanan siber yang dikembangkan oleh AICPA (2018) membantu perusahaan mengidentifikasi, menilai, dan mengkomunikasikan risiko ini secara lebih efektif.

Dari perspektif manajemen, pengungkapan yang lebih baik tentang risiko keamanan siber dapat meningkatkan kepercayaan di antara pelanggan dan pemasok, serta memperpanjang durasi hubungan bisnis. Hal ini sejalan dengan temuan Bauer et al. (2018) bahwa kualitas kontrol internal pemasok berkorelasi positif dengan durasi hubungan pelanggan-pemasok.

Penelitian ini menyoroti pentingnya pengungkapan risiko keamanan siber dalam membangun hubungan pelanggan-pemasok yang lebih kuat dan tahan terhadap ancaman siber. Dengan menggali literatur yang ada, penelitian ini memberikan wawasan tentang bagaimana transparansi dalam pengungkapan risiko dapat meningkatkan kepercayaan dan kinerja dalam rantai pasok. Di era di mana keamanan siber menjadi isu global yang semakin kompleks, perusahaan perlu mengambil langkah proaktif untuk mengintegrasikan pengelolaan risiko ini ke dalam strategi bisnis mereka.

KAJIAN PUSTAKA

Penelitian mengenai pengungkapan risiko keamanan siber telah menjadi topik penting dalam literatur akuntansi dan manajemen rantai pasok, terutama mengingat meningkatnya adopsi teknologi digital dalam berbagai sektor bisnis (Nelson & Wang, 2024). Cybersecurity disclosures (pengungkapan risiko keamanan siber) tidak hanya berdampak pada nilai pasar perusahaan, tetapi juga pada hubungan antara pelanggan dan pemasok dalam rantai pasok (Berkman et al., 2018; Amir, Shai, & Tsafrir, 2018). Kajian pustaka ini akan mengulas beberapa temuan utama dalam literatur yang terkait dengan pengungkapan risiko keamanan siber, hubungan pelanggan-pemasok, dan dampaknya terhadap efisiensi investasi serta kinerja organisasi.

Pengungkapan risiko keamanan siber memainkan peran penting dalam memberikan transparansi kepada pemangku kepentingan, termasuk pelanggan dan pemasok. AICPA (2018) menyoroti bahwa kerangka pelaporan risiko keamanan siber dapat meningkatkan kepercayaan mitra bisnis dengan memberikan wawasan tentang kesiapan perusahaan menghadapi ancaman siber. Hal ini sejalan dengan temuan Gordon et al. (2006), yang menyatakan bahwa pengungkapan yang lebih baik terkait aktivitas keamanan informasi dapat meningkatkan

persepsi pasar terhadap kredibilitas perusahaan. Nelson dan Wang (2024) menekankan bahwa perusahaan yang meningkatkan skor kesadaran keamanan siber cenderung mendapatkan peningkatan transaksi dari pelanggan utama mereka. Penelitian ini menggarisbawahi bahwa pengungkapan risiko siber dapat memitigasi asimetri informasi dan meningkatkan kepercayaan dalam hubungan pelanggan-pemasok.

Hubungan antara pelanggan dan pemasok dalam rantai pasok sangat dipengaruhi oleh kualitas pengendalian internal pemasok, termasuk kesiapan mereka terhadap risiko keamanan siber. Bauer et al. (2018) menemukan bahwa kualitas pengendalian internal pemasok berkorelasi positif dengan durasi hubungan pelanggan-pemasok. Dengan demikian, perusahaan yang mengungkapkan risiko keamanan siber secara transparan dapat memperpanjang hubungan mereka dengan pelanggan melalui peningkatan kepercayaan. Ashraf (2022) menambahkan bahwa pelanggaran data dapat menyebabkan dampak negatif pada reputasi perusahaan, yang pada gilirannya memengaruhi hubungan mereka dengan mitra rantai pasok. Penelitian ini menunjukkan bahwa peer events, seperti pelanggaran data pada perusahaan lain, dapat memicu perusahaan untuk memperkuat pengungkapan risiko mereka guna melindungi hubungan pelanggan-pemasok.

Keamanan siber juga berdampak pada efisiensi investasi dalam hubungan pelanggan-pemasok. Chiu, Kim, dan Wang (2019) menunjukkan bahwa pengungkapan risiko pelanggan dapat memengaruhi efisiensi investasi pemasok, terutama ketika ada ketidakpastian mengenai risiko pasar. Penelitian ini menyoroti pentingnya komunikasi yang jelas antara pelanggan dan pemasok terkait risiko yang mungkin memengaruhi keputusan investasi.

Chen et al. (2019) juga mengidentifikasi bahwa kualitas informasi linguistik dalam pengungkapan pelanggan memiliki dampak signifikan pada keputusan investasi pemasok. Perusahaan dengan pengungkapan risiko yang lebih berkualitas cenderung mendorong pemasok mereka untuk melakukan investasi yang lebih efisien dan terarah. Literatur juga mencatat dampak langsung dari ancaman siber pada nilai pasar perusahaan. Hinz et al. (2015) menunjukkan bahwa pencurian data dapat menyebabkan penurunan harga saham dan peningkatan risiko sistematis pada perusahaan di sektor elektronik konsumen. Hal ini sejalan dengan temuan Crosignani, Macchiavelli, dan Silva (2023), yang mengidentifikasi bahwa serangan siber dapat menyebar melalui rantai pasok, memengaruhi kinerja perusahaan secara keseluruhan. Richardson, Smith, dan Watson (2019) menambahkan bahwa dampak ekonomi dari pelanggaran data seringkali kurang signifikan daripada persepsi awal, terutama jika perusahaan memiliki mekanisme mitigasi yang memadai. Oleh karena itu, pengungkapan

risiko siber yang efektif dapat membantu perusahaan memitigasi dampak negatif dari ancaman ini.

Hubungan pelanggan-pemasok sering kali melibatkan investasi spesifik yang saling menguntungkan, tetapi juga berisiko tinggi jika salah satu pihak tidak memenuhi kewajiban mereka. Raman dan Shahrur (2008) menemukan bahwa investasi spesifik dalam hubungan ini dapat meningkatkan risiko manipulasi pendapatan, yang pada gilirannya memengaruhi kualitas hubungan. Namun, Chen et al. (2021) menunjukkan bahwa hubungan yang didasarkan pada koneksi personal dapat mengurangi asimetri informasi dan meningkatkan efisiensi. Penelitian Nelson (2018) mendukung pandangan ini dengan menyatakan bahwa kualitas informasi pelanggan utama dapat memengaruhi keputusan investasi pemasok, terutama dalam lingkungan yang penuh dengan ketidakpastian. Dengan demikian, pengungkapan risiko siber yang baik dapat menjadi alat penting untuk mengelola risiko dalam hubungan pelanggan-pemasok.

Regulasi memiliki peran penting dalam mendorong perusahaan untuk mengungkapkan risiko keamanan siber. Securities and Exchange Commission (SEC) (2011) mengeluarkan panduan tentang pengungkapan risiko siber, yang mendorong perusahaan untuk memberikan informasi yang lebih komprehensif kepada pemangku kepentingan mereka. Panduan ini telah membantu meningkatkan standar pengungkapan dan memperkuat kepercayaan antara pelanggan dan pemasok. Namun, McMillan (2017) mencatat bahwa banyak perusahaan enggan mengungkapkan pelanggaran keamanan karena kekhawatiran akan dampak reputasi. Hal ini menunjukkan perlunya insentif tambahan untuk mendorong perusahaan mengungkapkan risiko siber mereka secara transparan.

Kajian pustaka ini menunjukkan bahwa pengungkapan risiko keamanan siber memiliki dampak yang signifikan pada hubungan pelanggan-pemasok, efisiensi investasi, dan kinerja pasar perusahaan. Temuan ini menekankan pentingnya pengungkapan risiko siber yang transparan sebagai alat untuk membangun kepercayaan dan memitigasi risiko dalam rantai pasok. Dengan meningkatnya ancaman siber, penelitian lebih lanjut diperlukan untuk mengeksplorasi mekanisme yang dapat meningkatkan kualitas pengungkapan dan dampaknya pada hubungan pelanggan-pemasok.

METODOLOGI

Penelitian ini menggunakan pendekatan kualitatif dengan metode literatur review untuk mengkaji pengaruh pengungkapan risiko keamanan siber terhadap hubungan pelanggan-pemasok dalam rantai pasok perusahaan. Pendekatan ini dipilih karena memberikan pemahaman mendalam mengenai tema penelitian melalui analisis sistematis terhadap penelitian-penelitian terdahulu (Snyder, 2019). Literatur review sebagai metodologi memungkinkan peneliti untuk menyintesis berbagai studi yang relevan dengan topik tertentu dan mengevaluasi temuan dalam konteks teoritis yang lebih luas (Tranfield, Denyer, & Smart, 2003). Dalam penelitian ini, pendekatan sistematis digunakan untuk mengidentifikasi, memilih, dan menganalisis artikel ilmiah yang membahas pengungkapan risiko keamanan siber dan dampaknya terhadap hubungan pelanggan-pemasok.

Artikel yang digunakan dalam penelitian ini diambil dari database jurnal bereputasi. Kriteria inklusi mencakup penelitian yang diterbitkan dalam 10 tahun terakhir dan relevan dengan tema pengungkapan risiko keamanan siber serta rantai pasok (Snyder, 2019). Setiap artikel dianalisis untuk mengidentifikasi tema-tema utama yang terkait dengan hubungan pelanggan-pemasok dalam konteks pengungkapan risiko siber. Penelitian sebelumnya dibandingkan dan dikritisi untuk mengidentifikasi celah penelitian (Booth, Sutton, & Papaioannou, 2016).

Sumber data utama dalam penelitian ini adalah artikel jurnal akademik, laporan industri, dan kebijakan regulasi. Beberapa artikel kunci yang digunakan mencakup Nelson dan Wang (2024), yang menyoroti pentingnya pengungkapan risiko siber dalam memperkuat kepercayaan antara pelanggan dan pemasok, serta Crosignani, Macchiavelli, dan Silva (2023), yang membahas propagasi serangan siber melalui rantai pasok. Sebagai tambahan, data sekunder berupa laporan tahunan perusahaan, kebijakan regulasi seperti pedoman Cybersecurity Disclosure Guidance dari SEC (2011), dan laporan industri seperti Annual Cybersecurity Report oleh Cisco (2017) digunakan untuk melengkapi analisis.

Proses analisis data dilakukan melalui beberapa tahap yaitu 1) ekstraksi data adalah artikel yang relevan diekstraksi untuk mendapatkan informasi tentang variabel utama, seperti tingkat pengungkapan risiko siber, durasi hubungan pelanggan-pemasok, dan dampak serangan siber pada kinerja perusahaan; 2) koding tematik yaitu teknik koding digunakan untuk mengelompokkan temuan berdasarkan tema utama, seperti dampak keamanan siber pada efisiensi investasi dan kepercayaan mitra bisnis (Braun & Clarke, 2006); sintesis naratif yaitu temuan dari berbagai studi disintesis secara naratif untuk memberikan gambaran menyeluruh

tentang hubungan antara pengungkapan risiko siber dan manajemen rantai pasok (Popay et al., 2006).

Pendekatan literatur review memiliki kelebihan dalam menyediakan pemahaman yang komprehensif terhadap topik yang kompleks (Snyder, 2019). Namun, terdapat keterbatasan berupa potensi bias seleksi artikel dan ketergantungan pada data sekunder. Oleh karena itu, penelitian ini memastikan bahwa proses seleksi artikel dilakukan secara sistematis dengan menggunakan protokol yang jelas (Tranfield et al., 2003).

HASIL PENELITIAN

Penelitian ini bertujuan untuk mengeksplorasi dampak pengungkapan risiko keamanan siber terhadap hubungan pelanggan-pemasok dalam rantai pasok perusahaan melalui pendekatan kualitatif literatur review. Berdasarkan analisis terhadap berbagai literatur terkini, beberapa temuan utama dapat diidentifikasi sebagai berikut:

1. Pengaruh Pengungkapan Risiko Siber terhadap Kepercayaan dalam Hubungan Pelanggan-Pemasok.

   Pengungkapan risiko siber memainkan peran penting dalam membangun kepercayaan antara pelanggan dan pemasok. Menurut Nelson dan Wang (2024), perusahaan yang secara transparan mengungkapkan risiko siber kepada mitra mereka cenderung menciptakan hubungan yang lebih kokoh. Pengungkapan ini memberikan sinyal kepada mitra bisnis bahwa perusahaan memiliki kontrol internal yang memadai untuk menangani ancaman keamanan siber. Crosignani, Macchiavelli, dan Silva (2023) menekankan bahwa serangan siber yang tidak terungkap dapat menyebar melalui rantai pasok, menyebabkan dampak finansial dan reputasi yang signifikan. Oleh karena itu, pengungkapan yang efektif membantu memitigasi risiko tersebut dan meningkatkan loyalitas mitra bisnis. Dampak pada Investasi Khusus dalam Hubungan Pemasok. Studi sebelumnya menunjukkan bahwa pemasok lebih cenderung melakukan investasi spesifik hubungan jika pelanggan mereka memiliki tingkat transparansi yang tinggi dalam pengungkapan risiko siber. Chen (2022) menyatakan bahwa investasi khusus hubungan meningkat ketika pemasok yakin bahwa pelanggan mereka memiliki mekanisme untuk melindungi data dan operasional dari ancaman siber. Hal serupa ditemukan oleh Chiu, Kim, dan Wang (2019), yang menunjukkan bahwa pengungkapan risiko siber memengaruhi efisiensi investasi pemasok. Ketika risiko diungkapkan dengan jelas, pemasok memiliki informasi yang lebih baik untuk membuat keputusan investasi yang mendukung hubungan jangka panjang.

2. Dampak Keamanan Siber pada Stabilitas Hubungan Pelanggan-Pemasok.

   Keamanan siber juga berperan dalam stabilitas hubungan jangka panjang antara pelanggan dan pemasok. Bauer, Henderson, dan Lynch (2018) mencatat bahwa pemasok cenderung memperpanjang durasi hubungan dengan pelanggan yang memiliki kontrol internal berkualitas tinggi, termasuk pengelolaan risiko siber. Penelitian ini mendukung temuan bahwa pengungkapan risiko siber memperkuat stabilitas hubungan dengan memberikan rasa aman kepada mitra bisnis. Penelitian juga menunjukkan bahwa kegagalan dalam mengungkapkan risiko siber dapat berdampak buruk pada kinerja keuangan perusahaan. Berkman et al. (2018) menemukan bahwa perusahaan yang mengalami pelanggaran data tetapi gagal mengungkapkan risiko sebelumnya mengalami penurunan nilai pasar yang lebih besar dibandingkan perusahaan yang transparan. Dengan demikian, transparansi dalam pengungkapan risiko siber tidak hanya meningkatkan hubungan bisnis tetapi juga melindungi nilai ekonomi perusahaan. Peran regulasi dalam mendorong pengungkapan risiko siber juga menjadi sorotan penting. Menurut pedoman Cybersecurity Disclosure Guidance dari Securities and Exchange Commission (2011), perusahaan diharapkan untuk secara proaktif mengungkapkan potensi risiko siber dan tindakan mitigasi. Studi Haapamäki dan Sihvonen (2019) menunjukkan bahwa kepatuhan terhadap pedoman ini meningkatkan kepercayaan investor dan mitra bisnis, termasuk dalam konteks hubungan pelanggan-pemasok. Hasil penelitian menunjukkan bahwa pengungkapan risiko keamanan siber memiliki dampak yang signifikan terhadap hubungan pelanggan-pemasok. Pengungkapan ini tidak hanya meningkatkan kepercayaan dan stabilitas hubungan, tetapi juga mendorong investasi spesifik hubungan dan melindungi nilai ekonomi perusahaan. Studi ini menekankan pentingnya transparansi dan kepatuhan terhadap regulasi dalam pengungkapan risiko siber untuk memperkuat rantai pasok perusahaan.

PEMBAHASAN

Pembahasan ini menganalisis hasil penelitian tentang pengaruh pengungkapan risiko keamanan siber terhadap hubungan pelanggan-pemasok dalam rantai pasok perusahaan. Melalui pendekatan literatur review, penelitian ini mengeksplorasi dampak pengungkapan risiko siber terhadap kepercayaan, investasi hubungan, stabilitas relasi, dan kinerja ekonomi perusahaan. Sebagai pelengkap, penelitian terdahulu dibandingkan untuk memperkuat argumentasi.

Pengungkapan risiko siber memiliki dampak signifikan terhadap tingkat kepercayaan dalam hubungan pelanggan-pemasok. Nelson dan Wang (2024) menunjukkan bahwa transparansi dalam mengomunikasikan risiko siber membantu pelanggan dan pemasok memahami potensi ancaman serta strategi mitigasi yang diterapkan. Hal ini sejalan dengan penelitian oleh Martin, Borah, dan Palmatier (2017), yang menemukan bahwa perusahaan yang proaktif dalam mengelola risiko data cenderung memiliki kinerja pelanggan yang lebih baik karena meningkatnya rasa aman. Namun, Crosignani, Macchiavelli, dan Silva (2023) mengingatkan bahwa kepercayaan tidak hanya tergantung pada pengungkapan, tetapi juga pada kemampuan perusahaan untuk mencegah penyebaran ancaman melalui rantai pasoknya. Perbandingan ini menegaskan bahwa kepercayaan tidak hanya berbasis pada informasi yang diungkapkan, tetapi juga pada tindakan konkret untuk meminimalkan risiko.

Keputusan pemasok untuk melakukan investasi spesifik hubungan sangat bergantung pada transparansi pelanggan. Penelitian oleh Chen (2022) mengindikasikan bahwa pemasok lebih cenderung meningkatkan investasi jika pelanggan memberikan informasi risiko siber secara terbuka. Hal ini memperkuat temuan Chiu, Kim, dan Wang (2019), yang menyatakan bahwa pengungkapan risiko membantu pemasok mengalokasikan sumber daya secara efisien untuk meningkatkan hubungan strategis. Sebagai perbandingan, penelitian oleh Raman dan Shahrur (2008) menyoroti bahwa investasi spesifik hubungan juga dipengaruhi oleh komitmen finansial pelanggan terhadap keamanan data. Keterlibatan aktif dalam melindungi rantai pasok, seperti yang ditunjukkan dalam studi ini, memperkuat motivasi pemasok untuk berinvestasi lebih jauh.

Stabilitas hubungan pelanggan-pemasok dapat dipengaruhi secara signifikan oleh pengungkapan risiko siber. Bauer, Henderson, dan Lynch (2018) menemukan bahwa pemasok lebih memilih untuk mempertahankan hubungan jangka panjang dengan pelanggan yang memiliki kontrol internal yang memadai, termasuk pengelolaan risiko siber. Penelitian ini konsisten dengan temuan oleh Berkman et al. (2018), yang menunjukkan bahwa perusahaan dengan sistem keamanan yang kuat dan transparansi dalam pengungkapan risiko memiliki hubungan yang lebih stabil. Sebaliknya, studi oleh Richardson, Smith, dan Weidenmier Watson (2019) menyoroti bahwa kegagalan untuk mengungkapkan risiko dapat menciptakan ketidakpastian, yang berpotensi merusak hubungan. Dengan demikian, stabilitas relasi tidak hanya bergantung pada pengungkapan risiko tetapi juga pada langkah mitigasi yang nyata.

Pengungkapan risiko siber juga memiliki implikasi ekonomi yang luas. Menurut Berkman et al. (2018), perusahaan yang mengalami pelanggaran data tanpa pengungkapan sebelumnya mengalami penurunan nilai pasar yang signifikan. Hal ini berbeda dengan perusahaan yang secara aktif mengungkapkan risiko, yang cenderung menghadapi penurunan nilai pasar yang lebih kecil. Patatoukas (2012) menambahkan bahwa transparansi dalam pengungkapan risiko siber dapat meningkatkan akses perusahaan ke modal karena kepercayaan investor yang lebih besar. Namun, Hinz et al. (2015) berpendapat bahwa efek ekonomi tersebut tidak hanya berasal dari pengungkapan, tetapi juga dari efisiensi respons perusahaan terhadap ancaman siber.

Regulasi memiliki peran penting dalam mendorong pengungkapan risiko siber. Pedoman dari Securities and Exchange Commission (2011) dan American Institute of Certified Public Accountants (2018) menetapkan bahwa perusahaan harus proaktif dalam mengungkapkan risiko siber untuk memastikan transparansi dan akuntabilitas. Haapamäki dan Sihvonen (2019) menunjukkan bahwa perusahaan yang patuh pada regulasi ini lebih cenderung membangun hubungan pelanggan-pemasok yang kokoh. Namun, Shumsky (2016) mencatat bahwa beberapa perusahaan enggan mengungkapkan risiko siber karena khawatir akan dampak reputasional. Penelitian ini memberikan perspektif bahwa efektivitas regulasi bergantung pada insentif yang mendorong perusahaan untuk memprioritaskan transparansi. Risiko siber yang tidak dikelola dengan baik dapat menyebar melalui rantai pasok perusahaan. Crosignani, Macchiavelli, dan Silva (2023) menunjukkan bahwa serangan siber pada satu entitas dalam rantai pasok dapat memengaruhi seluruh ekosistem. Hal ini diperkuat oleh studi Zhou dan WC (2007), yang menyoroti pentingnya berbagi informasi keamanan dalam rantai pasok untuk mengurangi risiko propagasi. Namun, Martin et al. (2017) menunjukkan bahwa berbagi informasi ini harus dilakukan dengan hati-hati untuk melindungi kerahasiaan data. Perbedaan ini menunjukkan bahwa manajemen risiko siber dalam rantai pasok memerlukan keseimbangan antara transparansi dan keamanan.

Pengungkapan risiko siber dapat memengaruhi reputasi perusahaan di mata mitra bisnis dan pelanggan. Menurut Martin, Borah, dan Palmatier (2017), transparansi dalam pengungkapan risiko meningkatkan reputasi perusahaan sebagai entitas yang bertanggung jawab. Sebaliknya, penelitian oleh Richardson et al. (2019) menunjukkan bahwa kegagalan untuk mengungkapkan risiko dapat menyebabkan kerugian reputasi yang signifikan. Sebagai perbandingan, Gordon et al. (2006) menemukan bahwa reputasi perusahaan juga dipengaruhi oleh kecepatan dan efektivitas respons terhadap ancaman siber. Hal ini menekankan bahwa pengungkapan risiko saja tidak cukup tanpa tindakan yang sesuai untuk menangani ancaman.

Pengungkapan risiko keamanan siber memiliki dampak yang luas terhadap berbagai aspek hubungan pelanggan-pemasok dalam rantai pasok perusahaan. Penelitian ini menunjukkan bahwa transparansi dalam pengungkapan risiko dapat meningkatkan kepercayaan, mendorong investasi spesifik hubungan, memperkuat stabilitas relasi, dan melindungi nilai ekonomi perusahaan. Namun, efektivitas pengungkapan sangat tergantung pada konteks regulasi, kemampuan mitigasi, dan strategi komunikasi perusahaan. Perbandingan dengan penelitian terdahulu memberikan perspektif yang kaya tentang bagaimana pengungkapan risiko siber memengaruhi dinamika hubungan bisnis. Penelitian ini menyoroti pentingnya pendekatan holistik dalam manajemen risiko siber untuk mencapai keberlanjutan hubungan pelanggan-pemasok.

SIMPULAN

Penelitian ini menyimpulkan bahwa pengungkapan risiko keamanan siber memainkan peran krusial dalam membangun dan mempertahankan hubungan pelanggan-pemasok dalam rantai pasok perusahaan. Transparansi dalam pengungkapan risiko dapat meningkatkan kepercayaan antara mitra bisnis, mendorong investasi spesifik hubungan, dan memperkuat stabilitas relasi, sehingga berdampak positif pada kinerja ekonomi perusahaan secara keseluruhan. Namun, efektivitas pengungkapan risiko sangat bergantung pada langkah mitigasi yang diambil perusahaan, kepatuhan terhadap regulasi, dan strategi komunikasi yang diterapkan.

Hasil penelitian juga menunjukkan bahwa kegagalan dalam mengungkapkan risiko keamanan siber dapat menciptakan ketidakpastian, merusak reputasi, dan melemahkan hubungan dalam rantai pasok. Dengan demikian, manajemen risiko siber yang efektif memerlukan pendekatan yang holistik, mencakup transparansi informasi, perlindungan data, dan kerja sama strategis antara pelanggan dan pemasok.

LIMITASI

Meskipun penelitian ini memberikan wawasan yang berharga, terdapat beberapa limitasi yang perlu diperhatikan. Penelitian ini sepenuhnya didasarkan pada tinjauan literatur yang ada, sehingga terbatas pada data dan hasil dari penelitian terdahulu. Kurangnya data empiris primer dapat membatasi generalisasi hasil penelitian.

Literasi literatur yang digunakan berasal dari berbagai industri dengan tingkat risiko siber dan kompleksitas rantai pasok yang berbeda. Hal ini dapat memengaruhi relevansi hasil untuk sektor tertentu. Meskipun penelitian ini mengadopsi pendekatan global, sebagian besar

referensi berasal dari negara-negara maju. Hal ini dapat mengabaikan konteks spesifik negara berkembang yang mungkin memiliki tantangan dan peluang yang berbeda dalam mengelola risiko siber. Penelitian ini kurang mengeksplorasi bagaimana teknologi seperti kecerdasan buatan dan blockchain dapat memengaruhi pengungkapan dan mitigasi risiko siber dalam rantai pasok, padahal teknologi ini semakin relevan dalam konteks modern. Pengaruh pengungkapan risiko siber terhadap hubungan pelanggan-pemasok seringkali bersifat tidak langsung dan multidimensional, sehingga sulit diukur secara terpisah dari faktor lain yang memengaruhi hubungan tersebut.

Penelitian mendatang dapat mengatasi limitasi ini dengan: Melakukan studi empiris untuk menguji hubungan kausal antara pengungkapan risiko siber dan dinamika hubungan pelanggan-pemasok. Fokus pada sektor atau industri tertentu untuk mendapatkan temuan yang lebih spesifik dan relevan. Mengeksplorasi dampak teknologi baru terhadap manajemen risiko siber dan transparansi dalam rantai pasok. Memperluas perspektif geografis dengan mencakup lebih banyak studi dari negara berkembang. Dengan mengatasi keterbatasan tersebut, penelitian di masa depan dapat memberikan pandangan yang lebih komprehensif dan mendalam terkait pengungkapan risiko keamanan siber dan dampaknya pada rantai pasok perusahaan.

DAFTAR PUSTAKA

AICPA. (2018). *Cybersecurity risk management reporting fact sheet*. Retrieved from https://www.aicpa-cima.com/resources/download/why-use-the-aicpas-cybersecurity-risk-management-reporting-framework

Amir, E., Shai, L., & Tsafrir, L. (2018). Do firms underreport information on cyberattacks? *Review of Accounting Studies*, 23(3), 1177–1206.

Ashraf, M. (2022). The role of peer events in corporate governance: Evidence from data breaches. *The Accounting Review*, 97(2), 1–24.

Bauer, A. M., Henderson, D., & Lynch, D. P. (2018). Supplier internal control quality and the duration of customer-supplier relationships. *The Accounting Review*, 93(3), 59–82.

Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy*, 37(6), 508–526.

Booth, A., Sutton, A., & Papaioannou, D. (2016). *Systematic approaches to a successful literature review*. SAGE Publications.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Chen, C., Kim, J.-B., Wei, M., & Zhang, H. (2019). Linguistic information quality in customers' forward-looking disclosures and suppliers' investment decisions. *Contemporary Accounting Research*, 36(3), 1751–1783.

Chen, K. (2022). Suppliers' relationship-specific investments and customers' management forecasts. *Advances in Accounting*, 59, 100626.

Chiu, T.-T., Kim, J.-B., & Wang, Z. (2019). Customers' risk factor disclosures and suppliers' investment efficiency. *Contemporary Accounting Research*, 36(2), 773–804.

Crosignani, M., Macchiavelli, M., & Silva, A. F. (2023). Pirates without borders: The propagation of cyberattacks through firms' supply chains. *Journal of Financial Economics*, 147(2), 432–448.

Ekawahyu Kasih, Farah Qalbia, & Novrizal Novrizal. (2022). Empowering Talent In The Age Of Artificial Intelligence: Innovations In Human Resource Management. *The International Conference on Education, Social Sciences and Technology (ICESST)*, *1*(2), 287–295. https://doi.org/10.55606/icesst.v1i2.383

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Sohail, T. (2006). The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities. *Journal of Accounting and Public Policy*, 25(5), 503–530.

Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. *Managerial Auditing Journal*, 34(7), 808–834.

https://doi.org/10.1002/jcaf.22695

https://doi.org/10.1016/j.jbusres.2019.07.039

https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing*, 81(1), 36–58.

Nelson, A., & Wang, S. (2024). The importance of cybersecurity disclosures in customer relationships. *The Journal of Corporate Accounting & Finance.*

Popay, J., Roberts, H., Sowden, A., Petticrew, M., Arai, L., Rodgers, M., ... & Duffy, S. (2006). *Guidance on the conduct of narrative synthesis in systematic reviews*. A product from the ESRC Methods Programme.

Richardson, V. J., Smith, R. E., & Weidenmier Watson, M. (2019). Cybersecurity risk management: Oversight and disclosure. *The CPA Journal*, 89(4), 18–25.

Ruslaini Ruslaini, Dadang Irawan, Farah Qalbia, & Seger Santoso. (2022). Optimizing Human Capital in the Era of AI Advancements : Strategi for the Future Workforce. *The International Conference on Education, Social Sciences and Technology (ICESST)*, *1*(2), 278–286. https://doi.org/10.55606/icesst.v1i2.382

Securities and Exchange Commission (SEC). (2011). *CF disclosure guidance: Topic No. 2 cybersecurity*. Retrieved from

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, 104, 333–339.

Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a methodology for developing evidence-informed management knowledge by means of systematic review. *British Journal of Management*, 14(3), 207–222. https://doi.org/10.1111/1467-8551.00375