



Peran Asuransi Siber (*Cyber Insurance*) Sebagai Alat Transfer Risiko di Era Digital

Haura Rifqa Hascarjani¹, Yohana Tirta Widia Swari Simamora²

Simamorayohana95@gmail.com¹, haurarifga9@gmail.com²

¹²Universitas Negeri Medan

Article Info

Article history:

Received Jun 05th, 2026

Revised Jun 08th, 2026

Accepted Jun 10th, 2026

Kata Kunci:

Asuransi siber

Cyber insurance

Transfer risiko

Manajemen risiko

Risiko siber

Transformasi digital

ABSTRAK

Transformasi digital yang pesat meningkatkan ketergantungan organisasi terhadap teknologi informasi sekaligus memperbesar risiko ancaman siber seperti kebocoran data, *ransomware*, *malware*, dan gangguan sistem informasi yang dapat menimbulkan kerugian finansial, operasional, hukum, dan reputasi. Dalam manajemen risiko, salah satu strategi yang digunakan adalah transfer risiko melalui asuransi siber (*cyber insurance*). Penelitian ini bertujuan untuk menganalisis peran asuransi siber sebagai instrumen transfer risiko di era digital, mengidentifikasi manfaat dan keterbatasannya, serta mengkaji peluang pengembangannya dalam mendukung manajemen risiko organisasi. Penelitian ini menggunakan pendekatan kualitatif dengan metode *Systematic Literature Review (SLR)*. Hasil penelitian menunjukkan bahwa asuransi siber berperan dalam mengalihkan sebagian dampak finansial dari insiden siber serta mendorong peningkatan kesadaran keamanan informasi dan praktik manajemen risiko organisasi. Namun demikian, implementasinya masih menghadapi tantangan seperti kesulitan kuantifikasi risiko, korelasi risiko siber yang tinggi, keterbatasan cakupan polis, dan rendahnya pemahaman organisasi.

ABSTARCT

Rapid digital transformation is increasing organizations' reliance on information technology while simultaneously amplifying the risk of cyber threats such as data breaches, ransomware, malware, and information system disruptions, which can result in financial, operational, legal, and reputational losses. In risk management, one strategy employed is risk transfer through cyber insurance. This study aims to analyze the role of cyber insurance as a risk transfer instrument in the digital era, identify its benefits and limitations, and examine opportunities for its development in supporting organizational risk management. This study employs a qualitative approach using the Systematic Literature Review (SLR) method. The results indicate that cyber insurance plays a role in mitigating some of the financial impacts of cyber incidents and in promoting increased awareness of information security and organizational risk management practices. However, its implementation still faces challenges such as difficulties in quantifying risks, the high correlation of cyber risks, limitations in policy coverage, and a lack of organizational understanding.



© 2021 Para Penulis. Diterbitkan oleh Perkumpulan Konsultan Manajemen Pendidikan Indonesia (PKMPI). Ini adalah artikel akses terbuka di bawah lisensi CC BY-NC-SA (<https://creativecommons.org/licenses/by-nc-sa/4.0>)

Corresponding Author:

Haura Rifqa Hascarjani¹, Yohana Tirta Widia Swari Simamora²
Universitas Negeri Medan dan Indra Kasih, Medan
Email: haurarifqa9p2@gmail.com¹, yohanasimamora376@gmail.com²

Latar Belakang

Perkembangan Revolusi Industri 4.0 dan transformasi digital telah mendorong organisasi di berbagai sektor untuk semakin bergantung pada teknologi informasi dalam menjalankan aktivitas operasionalnya. Pemanfaatan sistem digital memberikan berbagai manfaat, seperti peningkatan efisiensi, produktivitas, dan kualitas layanan. Namun, di balik manfaat tersebut, organisasi juga menghadapi ancaman siber yang semakin kompleks, mulai dari pencurian data, malware, ransomware, hingga gangguan terhadap sistem informasi. Ancaman ini tidak hanya menimbulkan kerugian finansial, tetapi juga dapat merusak reputasi organisasi dan menurunkan kepercayaan pemangku kepentingan.

Tingginya risiko siber tercermin dari berbagai laporan global. IBM Security (2023) melaporkan bahwa rata-rata biaya pelanggaran data mencapai USD 4,45 juta per insiden, meningkat sekitar 15% dibandingkan tiga tahun sebelumnya. Sementara itu, *Cybersecurity Ventures* memproyeksikan kerugian ekonomi global akibat kejahatan siber mencapai USD 10,5 triliun per tahun pada 2025. Di Indonesia, berbagai kasus kebocoran data dan serangan *ransomware* yang menimpa institusi pemerintah, sektor kesehatan, dan lembaga keuangan menunjukkan bahwa risiko siber telah menjadi salah satu tantangan utama dalam pengelolaan organisasi modern.

Dalam perspektif manajemen risiko, organisasi dapat menerapkan berbagai strategi penanganan risiko, yaitu penghindaran risiko (*risk avoidance*), pengurangan risiko (*risk reduction*), penerimaan risiko (*risk acceptance*), dan transfer risiko (*risk transfer*). Meskipun berbagai pengendalian keamanan informasi telah diterapkan, tidak semua risiko siber dapat dihilangkan sepenuhnya. Oleh karena itu, diperlukan mekanisme yang mampu mengalihkan dampak finansial dari risiko residual kepada pihak lain. Salah satu instrumen yang berkembang pesat dalam beberapa tahun terakhir adalah asuransi siber (*cyber insurance*), yaitu produk asuransi yang dirancang untuk memberikan perlindungan terhadap kerugian yang timbul akibat insiden keamanan siber.

Sejumlah penelitian terdahulu telah membahas asuransi siber dari berbagai perspektif. Böhme dan Schwartz (2020) menyoroti tantangan pemodelan risiko siber dalam industri asuransi, sedangkan Biener, Eling, dan Wirfs (2021) menemukan bahwa keterbatasan data historis dan tingginya korelasi antar risiko menjadi hambatan utama dalam pengembangan asuransi siber. Marotta et al. (2021) menempatkan asuransi siber sebagai bagian dari manajemen risiko yang holistik, sementara Romanosky et al. (2021) menganalisis karakteristik polis asuransi siber dan mekanisme penetapan preminya. Meskipun demikian, kajian yang membahas secara komprehensif peran asuransi siber sebagai alat transfer risiko di tengah meningkatnya ancaman digital, khususnya dalam konteks organisasi di Indonesia, masih relatif terbatas.

Berdasarkan kondisi tersebut, penelitian ini bertujuan untuk menganalisis peran asuransi siber sebagai instrumen transfer risiko di era digital, mengidentifikasi manfaat dan keterbatasannya dalam pengelolaan risiko siber, serta mengkaji peluang dan tantangan implementasinya dalam mendukung ketahanan organisasi. Hasil penelitian diharapkan dapat memberikan kontribusi bagi pengembangan literatur manajemen risiko sekaligus menjadi referensi bagi organisasi dalam mengintegrasikan asuransi siber ke dalam strategi pengelolaan risiko yang lebih komprehensif.

1. Teori Manajemen Risiko (*Risk Management Theory*)

Manajemen risiko merupakan proses sistematis yang digunakan organisasi untuk mengidentifikasi, menganalisis, mengevaluasi, dan mengendalikan risiko yang dapat memengaruhi pencapaian tujuan organisasi. Menurut ISO 31000:2018, risiko didefinisikan sebagai efek ketidakpastian terhadap tujuan, sehingga pengelolaan risiko tidak hanya berfokus pada upaya

menghindari kerugian, tetapi juga memastikan organisasi mampu merespons berbagai ketidakpastian secara efektif. Dalam kerangka *Enterprise Risk Management (ERM)* yang dikembangkan oleh COSO, manajemen risiko dipandang sebagai bagian integral dari strategi dan tata kelola organisasi.

Perkembangan teknologi digital telah mengubah lanskap risiko yang dihadapi organisasi. Ketergantungan yang semakin tinggi terhadap sistem informasi, jaringan internet, komputasi awan, dan layanan digital menyebabkan munculnya berbagai risiko baru yang sebelumnya tidak dominan dalam aktivitas bisnis. Risiko-risiko tersebut tidak hanya berdampak pada aspek operasional, tetapi juga dapat memengaruhi kondisi keuangan, reputasi, dan keberlangsungan organisasi. Oleh karena itu, manajemen risiko di era digital menuntut pendekatan yang lebih adaptif dan terintegrasi untuk menghadapi ancaman yang terus berkembang.

Dalam praktiknya, terdapat empat strategi utama dalam penanganan risiko, yaitu penghindaran risiko (*risk avoidance*), pengurangan risiko (*risk reduction*), penerimaan risiko (*risk acceptance*), dan transfer risiko (*risk transfer*). Keempat strategi tersebut dapat digunakan secara bersamaan sesuai dengan karakteristik risiko yang dihadapi organisasi. Untuk risiko yang berpotensi menimbulkan kerugian besar namun sulit dihilangkan sepenuhnya, strategi transfer risiko menjadi alternatif yang banyak digunakan melalui mekanisme asuransi.

2. Teori Transfer Risiko (*Risk Transfer Theory*)

Transfer risiko merupakan salah satu strategi manajemen risiko yang dilakukan dengan mengalihkan sebagian atau seluruh dampak finansial suatu risiko kepada pihak lain melalui mekanisme kontraktual. Menurut Harrington dan Niehaus (2023), transfer risiko bertujuan untuk mengurangi ketidakpastian finansial yang dapat mengganggu stabilitas organisasi apabila suatu peristiwa merugikan terjadi.

Dalam konteks manajemen risiko modern, transfer risiko dapat dilakukan melalui berbagai instrumen, seperti kontrak kerja sama, jaminan, maupun asuransi. Di antara berbagai instrumen tersebut, asuransi merupakan bentuk transfer risiko yang paling banyak digunakan karena menyediakan mekanisme perlindungan yang jelas melalui pembayaran premi dan pemberian kompensasi atas kerugian yang terjadi.

Strategi transfer risiko menjadi sangat penting ketika organisasi menghadapi risiko dengan dampak finansial yang tinggi namun frekuensi kejadiannya relatif rendah. Dalam kondisi tersebut, biaya untuk menanggung risiko secara mandiri sering kali lebih besar dibandingkan biaya yang dikeluarkan untuk mengalihkan risiko kepada perusahaan asuransi. Oleh karena itu, transfer risiko melalui asuransi menjadi salah satu komponen penting dalam sistem manajemen risiko organisasi.

3. Asuransi Siber (*Cyber Insurance*)

Asuransi siber (*cyber insurance*) merupakan produk asuransi yang dirancang khusus untuk memberikan perlindungan terhadap kerugian yang timbul akibat insiden keamanan siber. Kehadiran asuransi siber merupakan respons terhadap meningkatnya ancaman digital yang tidak dapat sepenuhnya diatasi melalui pengendalian teknologi maupun prosedur keamanan internal.

Secara umum, perlindungan dalam asuransi siber terbagi menjadi dua kategori utama. Pertama, *first-party coverage* yang memberikan perlindungan terhadap kerugian yang dialami langsung oleh tertanggung, seperti biaya pemulihan data, investigasi forensik digital, gangguan operasional, pembayaran tebusan ransomware, dan pemulihan reputasi perusahaan. Kedua, *third-party liability coverage* yang memberikan perlindungan terhadap tuntutan hukum atau kerugian pihak ketiga akibat kebocoran data maupun kegagalan sistem keamanan yang dimiliki organisasi.

Selain memberikan perlindungan finansial, asuransi siber juga memiliki fungsi preventif. Banyak perusahaan asuransi mensyaratkan penerapan standar keamanan tertentu sebelum memberikan perlindungan kepada calon tertanggung. Dengan demikian, asuransi siber tidak hanya berperan sebagai mekanisme transfer risiko, tetapi juga mendorong peningkatan kesadaran dan kualitas manajemen keamanan informasi dalam organisasi.

4. Risiko Siber (*Cyber Risk*)

Risiko siber (*cyber risk*) merupakan risiko yang timbul akibat kegagalan, penyalahgunaan, atau serangan terhadap sistem teknologi informasi dan komunikasi yang digunakan oleh organisasi. OECD (2021) mendefinisikan risiko siber sebagai potensi kerugian ekonomi, gangguan operasional, maupun kerusakan reputasi yang disebabkan oleh ancaman terhadap aset digital dan informasi.

Berbeda dengan risiko konvensional, risiko siber memiliki karakteristik yang unik. Pertama, ancaman siber berkembang sangat cepat seiring dengan kemajuan teknologi sehingga pola serangannya sulit diprediksi. Kedua, risiko siber memiliki tingkat keterkaitan yang tinggi karena suatu serangan dapat menyebar ke banyak organisasi melalui jaringan digital yang saling terhubung. Ketiga, sebagian besar aset yang menjadi target serangan, seperti data pelanggan dan informasi strategis perusahaan, bersifat tidak berwujud (*intangible*) sehingga nilai kerugiannya sulit diukur secara pasti.

Risiko siber dapat diklasifikasikan ke dalam beberapa kategori, yaitu risiko operasional akibat gangguan sistem, risiko data akibat kebocoran atau pencurian informasi, risiko keuangan akibat penipuan digital dan ransomware, risiko reputasi akibat hilangnya kepercayaan publik, serta risiko kepatuhan yang muncul karena pelanggaran regulasi perlindungan data. Kompleksitas risiko tersebut menyebabkan organisasi memerlukan pendekatan pengelolaan risiko yang lebih komprehensif dibandingkan dengan risiko tradisional.

5. Regulasi dan Perkembangan Asuransi Siber di Indonesia

Perkembangan asuransi siber tidak dapat dipisahkan dari perubahan regulasi yang mengatur keamanan informasi dan perlindungan data pribadi. Di Indonesia, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menjadi landasan hukum penting yang mengatur kewajiban organisasi dalam melindungi data pribadi serta memberikan sanksi terhadap pelanggaran yang terjadi.

Selain itu, sektor jasa keuangan juga diwajibkan menerapkan manajemen risiko teknologi informasi melalui berbagai regulasi yang diterbitkan oleh Otoritas Jasa Keuangan (OJK). Regulasi tersebut mendorong organisasi untuk meningkatkan kesiapan menghadapi ancaman siber serta memperkuat sistem pengelolaan risiko yang dimiliki.

Meskipun belum terdapat aturan yang secara khusus mewajibkan kepemilikan asuransi siber, meningkatnya tuntutan kepatuhan regulasi dan besarnya potensi kerugian akibat insiden siber menjadikan asuransi siber semakin relevan sebagai bagian dari strategi manajemen risiko organisasi. Oleh karena itu, keberadaan asuransi siber dipandang sebagai salah satu instrumen yang dapat membantu organisasi meningkatkan ketahanan dan keberlanjutan bisnis di era digital.

Metode Penelitian

Penelitian ini menggunakan pendekatan kualitatif dengan metode *Systematic Literature Review (SLR)*. Data yang digunakan dalam penelitian ini merupakan data sekunder yang diperoleh dari berbagai sumber ilmiah dan dokumen pendukung. Sumber data meliputi jurnal nasional dan internasional yang membahas manajemen risiko, risiko siber, dan asuransi siber, laporan industri dari lembaga seperti *IBM Security*, *Allianz*, dan *Cybersecurity Ventures*, serta regulasi dan pedoman resmi yang diterbitkan oleh organisasi internasional maupun lembaga pemerintah terkait. Analisis data dilakukan secara kualitatif melalui proses reduksi data, penyajian data, dan penarikan kesimpulan. Tahapan analisis ini mengacu pada pendekatan analisis data kualitatif yang dijelaskan oleh Matthew B. Miles, A. Michael Huberman, dan Johnny Saldaña yang kemudian disesuaikan dengan karakteristik penelitian studi literatur. Proses analisis dilakukan dengan mengidentifikasi informasi yang relevan dari berbagai sumber, mengelompokkan temuan berdasarkan tema yang sama, membandingkan hasil antar literatur, serta menyusun sintesis untuk memperoleh pemahaman yang komprehensif mengenai peran asuransi siber sebagai alat transfer risiko di era digital.

Hasil dan Pembahasan

Tren Peningkatan Risiko Siber di Era Digital

Hasil kajian terhadap berbagai literatur menunjukkan bahwa peningkatan penggunaan teknologi digital telah diikuti oleh peningkatan risiko keamanan siber yang signifikan. Risiko siber tidak lagi terbatas pada pencurian data atau peretasan sistem, tetapi telah berkembang menjadi ancaman yang dapat memengaruhi keberlangsungan organisasi secara keseluruhan. Berbagai penelitian menunjukkan bahwa serangan ransomware, phishing, malware, pencurian identitas

digital, hingga kebocoran data menjadi bentuk ancaman yang paling sering dialami organisasi dalam beberapa tahun terakhir.

Temuan ini menunjukkan bahwa risiko siber memiliki karakteristik yang berbeda dibandingkan risiko konvensional. Risiko siber bersifat dinamis, berkembang sangat cepat, dan mampu menimbulkan dampak lintas sektor dalam waktu yang relatif singkat. Franke (2017) menjelaskan bahwa risiko siber memiliki tingkat ketidakpastian yang tinggi karena pola serangan terus berubah mengikuti perkembangan teknologi. Selain itu, sifat keterhubungan (*interconnectedness*) dalam sistem digital menyebabkan satu insiden dapat berdampak pada banyak organisasi sekaligus.

Hasil kajian juga menunjukkan bahwa transformasi digital yang semakin masif memperbesar ketergantungan organisasi terhadap aset digital. Aset yang sebelumnya berbentuk fisik kini bertransformasi menjadi data, aplikasi, jaringan, dan sistem informasi yang menjadi target utama serangan siber. Akibatnya, kerugian yang ditimbulkan tidak hanya berupa kehilangan aset keuangan, tetapi juga mencakup gangguan operasional, hilangnya kepercayaan pelanggan, penurunan reputasi, serta risiko hukum akibat pelanggaran perlindungan data.

Temuan tersebut memperkuat pandangan bahwa ancaman siber telah berkembang menjadi risiko strategis organisasi. Risiko siber tidak lagi dipandang sebagai tanggung jawab divisi teknologi informasi semata, tetapi menjadi bagian dari manajemen risiko perusahaan yang harus dikelola secara terintegrasi oleh seluruh pemangku kepentingan organisasi.

Asuransi Siber Sebagai Mekanisme Transfer Risiko

Hasil analisis literatur menunjukkan bahwa asuransi siber berkembang sebagai respons terhadap meningkatnya kebutuhan organisasi untuk mengelola risiko residual yang tidak dapat dihilangkan melalui pengendalian internal. Dalam kerangka manajemen risiko, organisasi pada dasarnya dapat memilih untuk menghindari, mengurangi, menerima, atau mentransfer risiko. Namun, pada risiko siber yang memiliki potensi kerugian sangat besar, transfer risiko menjadi salah satu alternatif yang paling relevan.

Berbagai literatur menjelaskan bahwa mekanisme transfer risiko melalui asuransi siber dilakukan dengan mengalihkan sebagian konsekuensi finansial akibat insiden siber kepada perusahaan asuransi melalui pembayaran premi. Organisasi tetap bertanggung jawab dalam menerapkan pengendalian keamanan informasi, tetapi apabila insiden tetap terjadi, sebagian kerugian dapat ditanggung oleh perusahaan asuransi sesuai ketentuan polis yang berlaku.

Hasil sintesis menunjukkan bahwa asuransi siber modern tidak hanya berfungsi sebagai instrumen penggantian kerugian. Produk asuransi siber saat ini telah berkembang menjadi layanan manajemen risiko yang mencakup pendampingan respons insiden, investigasi forensik digital, konsultasi hukum, hingga pemulihan reputasi organisasi. Perkembangan ini menunjukkan adanya perubahan paradigma dari sekadar transfer risiko menjadi pendekatan yang lebih komprehensif dalam pengelolaan risiko siber.

Temuan ini sejalan dengan penelitian Romanosky et al. (2019) yang menyatakan bahwa asuransi siber telah berevolusi dari produk perlindungan sederhana menjadi bagian dari strategi ketahanan organisasi. Dengan kata lain, fungsi asuransi siber tidak hanya bersifat reaktif setelah insiden terjadi, tetapi juga memiliki kontribusi preventif dalam meningkatkan kesiapan organisasi menghadapi ancaman digital.

Bentuk Perlindungan Yang Diberikan Asuransi Siber

Berdasarkan hasil pengelompokan literatur, perlindungan asuransi siber dapat dibagi menjadi dua kategori utama, yaitu perlindungan terhadap kerugian yang dialami langsung oleh organisasi (*first-party coverage*) dan perlindungan terhadap tuntutan pihak ketiga (*third-party liability coverage*).

Perlindungan pihak pertama umumnya mencakup biaya pemulihan data dan sistem, investigasi forensik digital, biaya notifikasi kepada pelanggan yang terdampak, biaya pemulihan operasional, serta kerugian akibat penghentian aktivitas bisnis. Literatur menunjukkan bahwa biaya gangguan operasional menjadi salah satu komponen kerugian terbesar yang dialami organisasi setelah serangan siber.

Sementara itu, perlindungan pihak ketiga mencakup biaya litigasi, tuntutan hukum, denda regulasi, dan kompensasi kepada pihak yang dirugikan akibat kebocoran data. Aspek ini menjadi semakin penting setelah banyak negara menerapkan regulasi perlindungan data yang memberikan sanksi tegas terhadap organisasi yang gagal menjaga keamanan informasi pelanggan.

Hasil analisis menunjukkan bahwa cakupan perlindungan yang semakin luas menjadi salah satu alasan meningkatnya minat organisasi terhadap asuransi siber. Organisasi tidak hanya memperoleh perlindungan terhadap kerugian langsung, tetapi juga mendapatkan dukungan dalam menghadapi konsekuensi hukum dan reputasi yang muncul akibat insiden siber.

Manfaat Asuransi Siber Dalam Pengelolaan Risiko Organisasi

Hasil literatur mengidentifikasi empat manfaat utama asuransi siber, yaitu manfaat finansial, operasional, hukum, dan strategis.

Dari sisi finansial, asuransi siber membantu organisasi mengurangi dampak ekonomi akibat insiden siber. Biaya pemulihan sistem, kehilangan pendapatan selama gangguan operasional, hingga biaya investigasi dapat ditanggung sesuai cakupan polis. Kondisi ini membantu organisasi mempertahankan stabilitas keuangan ketika menghadapi serangan siber yang berdampak besar.

Dari sisi operasional, keberadaan asuransi siber memungkinkan organisasi memperoleh akses terhadap berbagai layanan profesional, seperti tim forensik digital, konsultan keamanan siber, dan layanan respons insiden. Keberadaan layanan tersebut mempercepat proses pemulihan dan mengurangi waktu penghentian operasional organisasi.

Dari sisi hukum, asuransi siber membantu organisasi menghadapi risiko tuntutan hukum akibat kebocoran data atau pelanggaran privasi. Temuan ini menjadi semakin relevan setelah munculnya berbagai regulasi perlindungan data yang memberikan kewajiban lebih besar kepada organisasi untuk menjaga keamanan informasi.

Manfaat yang paling menarik dari hasil penelitian ini adalah munculnya efek disiplin (*disciplining effect*). Beberapa penelitian menunjukkan bahwa perusahaan asuransi umumnya mensyaratkan penerapan standar keamanan tertentu sebelum memberikan perlindungan. Akibatnya, organisasi terdorong untuk meningkatkan kualitas sistem keamanan informasi, melakukan pelatihan keamanan siber, serta memperkuat tata kelola risiko. Dengan demikian, asuransi siber tidak hanya mengurangi dampak risiko, tetapi juga mendorong upaya pencegahan risiko.

Manfaat Asuransi Siber Dalam Pengelolaan Risiko Organisasi

Meskipun menawarkan berbagai manfaat, hasil kajian menunjukkan bahwa implementasi asuransi siber masih menghadapi berbagai tantangan yang cukup kompleks. Tantangan pertama adalah kesulitan dalam mengukur tingkat risiko siber secara akurat. Tidak seperti risiko tradisional yang memiliki data historis yang relatif stabil, ancaman siber terus berkembang sehingga menyulitkan proses perhitungan premi dan estimasi kerugian.

Tantangan kedua adalah tingginya korelasi risiko siber. Satu serangan dapat memengaruhi ribuan organisasi dalam waktu yang sama sehingga meningkatkan beban klaim perusahaan asuransi. Kondisi ini berbeda dengan risiko kebakaran atau kecelakaan yang umumnya terjadi secara individual dan tidak saling berkaitan.

Tantangan ketiga berkaitan dengan masalah moral hazard dan adverse selection. Organisasi yang telah memiliki perlindungan asuransi berpotensi mengurangi investasinya pada keamanan siber, sedangkan organisasi dengan tingkat risiko tinggi cenderung lebih aktif membeli asuransi. Kedua kondisi tersebut dapat meningkatkan risiko bagi perusahaan asuransi.

Selain itu, hasil kajian juga menunjukkan adanya kesenjangan pemahaman mengenai cakupan polis. Banyak organisasi menganggap seluruh kerugian akibat serangan siber akan ditanggung oleh perusahaan asuransi, padahal dalam praktiknya terdapat berbagai pengecualian yang dapat membatasi pembayaran klaim. Kondisi ini sering menjadi sumber sengketa antara tertanggung dan penanggung.

Implikasi Pengembangan Asuransi Siber di Indonesia

Dalam konteks Indonesia, hasil analisis menunjukkan bahwa potensi pengembangan asuransi siber masih sangat besar. Transformasi digital yang berlangsung pada sektor pemerintahan, perbankan, pendidikan, kesehatan, dan perdagangan elektronik menyebabkan eksposur terhadap risiko siber terus meningkat. Di sisi lain, tingkat pemanfaatan asuransi siber masih relatif rendah dibandingkan negara-negara maju.

Pemberlakuan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi menjadi faktor yang semakin memperkuat urgensi pengelolaan risiko siber. Organisasi yang mengalami kebocoran data kini menghadapi konsekuensi hukum dan finansial yang lebih besar

dibandingkan sebelumnya. Oleh karena itu, kebutuhan terhadap mekanisme transfer risiko diperkirakan akan terus meningkat.

Berdasarkan hasil literatur, pengembangan asuransi siber di Indonesia memerlukan dukungan dari berbagai pihak, termasuk regulator, perusahaan asuransi, penyedia layanan keamanan siber, dan organisasi pengguna. Kolaborasi tersebut diperlukan untuk meningkatkan literasi risiko siber, memperjelas regulasi, memperluas cakupan produk asuransi, serta menciptakan ekosistem manajemen risiko digital yang lebih matang.

Secara keseluruhan, penelitian ini menunjukkan bahwa asuransi siber memiliki peran penting sebagai alat transfer risiko di era digital. Namun, efektivitasnya akan lebih optimal apabila digunakan sebagai bagian dari strategi manajemen risiko yang terintegrasi dengan pengendalian teknis, kebijakan keamanan informasi, serta peningkatan kesadaran keamanan siber dalam organisasi.

Kesimpulan

Berdasarkan hasil analisis dan pembahasan yang telah dilakukan, dapat disimpulkan bahwa perkembangan transformasi digital telah meningkatkan risiko siber yang dihadapi organisasi di berbagai sektor. Ancaman seperti kebocoran data, ransomware, malware, dan gangguan sistem informasi tidak hanya menimbulkan kerugian finansial, tetapi juga berdampak pada aspek operasional, hukum, dan reputasi organisasi. Kondisi tersebut menjadikan risiko siber sebagai salah satu risiko strategis yang memerlukan pengelolaan secara komprehensif.

Hasil penelitian menunjukkan bahwa asuransi siber (cyber insurance) memiliki peran penting sebagai instrumen transfer risiko dalam kerangka manajemen risiko modern. Melalui mekanisme asuransi, organisasi dapat mengalihkan sebagian dampak finansial akibat insiden siber kepada perusahaan asuransi sesuai dengan ketentuan polis yang berlaku. Selain memberikan perlindungan terhadap kerugian langsung maupun tanggung jawab kepada pihak ketiga, asuransi siber juga berkontribusi dalam meningkatkan kualitas tata kelola risiko melalui penerapan standar keamanan informasi yang lebih baik.

Penelitian ini juga menemukan bahwa manfaat asuransi siber tidak hanya terbatas pada aspek finansial, tetapi mencakup manfaat operasional, hukum, dan strategis. Namun demikian, efektivitas asuransi siber masih menghadapi berbagai tantangan, antara lain kesulitan dalam mengukur tingkat risiko siber secara akurat, tingginya korelasi risiko antar organisasi, adanya kesenjangan antara ekspektasi perlindungan dan cakupan polis, serta rendahnya tingkat literasi dan adopsi asuransi siber, khususnya di Indonesia.

Oleh karena itu, asuransi siber tidak dapat dipandang sebagai solusi tunggal dalam menghadapi ancaman digital. Asuransi siber harus diintegrasikan dengan berbagai upaya pengendalian risiko lainnya, seperti penguatan keamanan teknologi informasi, peningkatan kesadaran keamanan siber sumber daya manusia, penerapan tata kelola keamanan informasi, dan kepatuhan terhadap regulasi yang berlaku. Dengan pendekatan yang terintegrasi tersebut, asuransi siber dapat berfungsi secara optimal sebagai alat transfer risiko sekaligus mendukung ketahanan organisasi dalam menghadapi tantangan keamanan siber di era digital.

Daftar Pustaka

- Allianz Global Corporate & Specialty. (2023). Allianz risk barometer 2023. Allianz SE. <https://www.allianz.com>
- Alya, B. Z., Hanum, F., & Rizal, M. (2026). Peran Teknologi Informasi dalam Pengembangan Sistem Informasi Akuntansi dalam Meningkatkan Kinerja Perusahaan: Studi Literatur tahun 2023-2025. *Jurnal Ilmu Ekonomi dan Bisnis*, 4(1), 18-26.
- Biener, C., Eling, M., & Wirfs, J. (2021). Insurability of cyber risk: An empirical analysis. *The Geneva Papers on Risk and Insurance – Issues and Practice*, 46(1), 1–25. <https://doi.org/10.1057/s41288-020-00200-7>
- Böhme, R., & Schwartz, G. (2020). Modeling cyber risk insurance. *Journal of Cybersecurity*, 6(1), 1–14. <https://doi.org/10.1093/cybsec/tyaa011>
- Cybersecurity Ventures. (2023). Cybercrime to cost the world \$10.5 trillion annually by 2025. <https://cybersecurityventures.com>

- Deloitte. (2023). Future of cyber insurance and risk transfer. Deloitte Insights. <https://www2.deloitte.com>
- ENISA. (2023). ENISA threat landscape 2023. European Union Agency for Cybersecurity. <https://www.enisa.europa.eu>
- Harrington, S. E., & Niehaus, G. (2023). Risk management and insurance (3rd ed.). McGraw-Hill Education.
- IBM Security. (2023). Cost of a data breach report 2023. IBM Corporation. <https://www.ibm.com/security/data-breach>
- ISO. (2022). ISO 31000:2018 risk management guidelines. International Organization for Standardization. <https://www.iso.org>
- KPMG. (2022). Cyber risk and insurance survey report. <https://kpmg.com>
- Marotta, A., Martinelli, F., Nanni, S., Orlando, A., & Yautsiukhin, A. (2021). Cyber insurance: State of the art, challenges, and future directions. *Computers & Security*, 108, 102–395. <https://doi.org/10.1016/j.cose.2021.102395>
- Munich Re. (2023). Cyber risk and insurance trends. <https://www.munichre.com>
- NIST. (2022). Cybersecurity framework (CSF 2.0 draft). National Institute of Standards and Technology. <https://www.nist.gov>
- OECD. (2021). Cyber risk insurance: Policy framework and market development. OECD Publishing. <https://www.oecd.org>
- Otoritas Jasa Keuangan. (2022). Peraturan OJK tentang penerapan manajemen risiko teknologi informasi. <https://www.ojk.go.id>
- PwC. (2024). Global digital trust insights 2024. PricewaterhouseCoopers. <https://www.pwc.com>
- Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2021). Content analysis of cyber insurance policies: How do insurers price cyber risk? *Journal of Cyber Policy*, 6(2), 1–25. <https://doi.org/10.1080/23738871.2021.1891764>
- Statista. (2024). Average cost of data breaches worldwide. <https://www.statista.com>
- UNCTAD. (2022). Digital economy report 2022. United Nations Conference on Trade and Development. <https://unctad.org>
- World Economic Forum. (2023). Global cyber security outlook 2023. <https://www.weforum.org>