DAMPAK FINANSIAL SERANGAN SIBER TERHADAP KINERJA KORPORASI: SCOPING REVIEW

Zakir Yusuf Gunibala[1]; Satia Nur Maharani[2]; Sri Pujiningsih[3]

Universitas Negeri Malang
Jln. Semarang No. 5, Malang, Jawa Timur
E-mail : zakir.yusuf.2304218@students.um.ac.id (Koresponding)

Submit: 29 Mei 2025 Review: 30 Juni 2025 Publish: 26 Juni 2025

Abstract: Rapid digital development has improved the operational efficiency of companies, but also increased exposure to the risk of cyber-attacks that can have a financial impact. This study aims to map and analyze the literature addressing the financial impact of cyberattacks on companies across sectors through a scoping review approach. The review process was based on the framework of Arksey and O'Malley (2005), including five stages: identification of research questions, search for relevant literature, selection of articles, data mapping, and preparation and reporting of results. A total of 10 selected scientific articles were analyzed and grouped into four main themes: (1) financial impacts and costs and (2) financial market reactions to cyberattacks. The findings show that cyberattacks cause real financial losses, including reduced stock prices, recovery costs, and reputational damage. The impact varies depending on industry sector, security readiness level, and transparency of incident reporting. The study also found gaps in cost estimation methodologies and incident reporting limitations that make comparative assessments between studies difficult. Therefore, future research should develop a standardized cost estimation approach, expand the geographical context of the study, and examine the long-term impact of cyberattacks on the financial sustainability of companies.

Keywords: *scoping review, cyber attack, financial impact, company loss, information security*

Perkembangan teknologi digital telah memberikan kemudahan luar biasa bagi aktivitas bisnis dan operasional perusahaan. Namun, kemajuan ini turut membawa risiko baru, yaitu ancaman serangan siber yang semakin kompleks, masif, dan terorganisir. Serangan siber tidak lagi hanya menyerang sistem informasi teknologi, tetapi secara langsung berdampak pada stabilitas dan keberlanjutan keuangan perusahaan. Berbagai laporan industri dan studi akademik menunjukkan bahwa insiden siber telah menjadi salah satu ancaman utama dalam pengelolaan risiko korporasi (Gordon et al., 2011).

Transformasi digital dalam dunia bisnis telah mempermudah jalannya proses operasional perusahaan dan memberikan dampak positif terhadap peningkatan kinerja. Studi menunjukkan bahwa perusahaan yang telah mengadopsi digitalisasi cenderung memiliki performa yang secara signifikan lebih unggul dibandingkan dengan perusahaan non-digital (Hossain & Sultana, 2024). Berbagai platform seperti e-commerce, layanan perbankan, dan sistem pemerintahan digital memiliki peran krusial dalam memperluas jangkauan pelayanan, meningkatkan interaksi dengan pengguna, serta memberikan layanan yang lebih efisien kepada masyarakat (Kitsing, 2017; Pawar & Palivela, 2022). Di sisi lain, kemudahan akses terhadap internet mendorong banyak individu untuk memulai usaha sendiri dan menjangkau konsumen global, yang turut mendorong pertumbuhan ekonomi dan mendukung upaya pengentasan kemiskinan (Thomas & Sule, 2023). Meski demikian, di balik manfaat besar dari teknologi informasi dan komunikasi (TIK), terdapat pula risiko yang menyertai, terutama dalam aspek keamanan siber yang rentan terhadap berbagai ancaman (Fonseca-Herrera et al., 2021; Jang-Jaccard & Nepal, 2014; Sotamaa et al., 2023)

Dampak finansial menjadi salah satu konsekuensi paling nyata dari serangan siber terhadap perusahaan. Kerugian ini mencakup biaya langsung seperti investigasi, pemulihan sistem, litigasi

hukum, dan kompensasi kepada pihak terdampak, serta kerugian tidak langsung seperti penurunan nilai saham, hilangnya pelanggan, dan berkurangnya kepercayaan investor (Kamiya et al., 2021; Romanosky, 2016). Studi empiris menunjukkan bahwa reaksi pasar terhadap insiden siber bersifat signifikan dan seringkali negatif, terutama pada hari-hari awal setelah pengungkapan insiden (Tosun, 2021). Hal ini mengindikasikan bahwa serangan siber tidak hanya menjadi masalah teknologi, tetapi juga menjadi isu strategis yang berimplikasi langsung pada kinerja finansial perusahaan.

Namun demikian, masih terdapat kesenjangan dalam pengetahuan dan literasi keuangan yang berkaitan dengan serangan siber, baik dari sisi akademik maupun praktis. Banyak perusahaan, khususnya di negara berkembang, belum memiliki pendekatan terstruktur dalam menilai dan mengantisipasi dampak finansial dari insiden siber. Bahkan, dalam beberapa kasus, serangan siber tidak dilaporkan secara terbuka karena kekhawatiran terhadap dampak reputasional, yang pada akhirnya mengaburkan pemahaman publik dan ilmiah tentang besarnya kerugian aktual (Meisner, 2018). Di sisi lain, sebagian besar studi fokus pada dampak teknis dan operasional, sementara konsekuensi keuangan kerap kali tidak dikaji secara mendalam atau dilaporkan secara tidak konsisten antar studi.

Dampak finansial dari serangan siber bisa sangat beragam dan signifikan. Kerugian tersebut dapat mencakup biaya investigasi forensik, pemberitahuan pelanggaran kepada pelanggan, biaya litigasi, penalti hukum, penguatan sistem keamanan, hingga penurunan nilai saham dan kerusakan reputasi (Shameli-Sendi et al., 2016). Konsekuensi finansial ini tidak hanya berdampak jangka pendek, tetapi juga berpotensi mengganggu keberlanjutan bisnis dan menurunkan kepercayaan investor. Di tengah tingginya frekuensi serangan dan kompleksitas bentuk kerugian yang ditimbulkan, perusahaan dituntut untuk lebih cermat dalam menilai serta memitigasi risiko keuangan yang timbul dari insiden siber.

Sejumlah penelitian telah mengkaji aspek teknis maupun strategis dari serangan siber, namun fokus kajian pada dampak finansial secara sistematis masih terbatas. Literatur yang ada belum secara komprehensif memetakan berbagai jenis kerugian finansial yang dialami perusahaan, baik yang bersifat langsung maupun tidak langsung. Selain itu, belum terdapat konsensus yang kuat mengenai pendekatan yang digunakan dalam mengukur dan mengevaluasi dampak finansial dari insiden tersebut. Hal ini menyebabkan kesenjangan dalam pengambilan keputusan strategis, khususnya dalam konteks manajemen risiko dan akuntabilitas perusahaan terhadap pemangku kepentingan.

Oleh karena itu, studi ini bertujuan untuk melakukan scoping review terhadap literatur yang membahas dampak finansial serangan siber terhadap perusahaan. Pendekatan scoping review sangat relevan untuk digunakan dalam konteks ini, karena memungkinkan peneliti untuk mengeksplorasi cakupan, tren, dan celah penelitian dalam bidang yang masih Studi ini diharapkan dapat memberikan kontribusi teoritis dalam memperluas pemahaman multidisipliner antara akuntansi, manajemen risiko, dan keamanan informasi, serta memberikan dasar praktis bagi manajemen perusahaan dan regulator untuk menyusun strategi mitigasi risiko siber secara lebih akuntabel dan berbasis bukti.

METODE

Tinjauan pelingkupan ini mengadopsi pendekatan yang dikembangkan oleh Arksey dan O'Malley (2005), yang mencakup lima tahapan utama, yaitu: (1) merumuskan pertanyaan penelitian, (2) mengidentifikasi studi yang relevan, (3) menyeleksi artikel, (4) memetakan data, serta (5) menyusun, merangkum, dan menyajikan temuan secara sistematis.

Identifikasi Pertanyaan Penelitian

Pertanyaan penelitian sangat penting untuk memandu arah bahasan dalam

penelitian ini. Sebagaimana topik tinjauan ini berkaitan dengan dampak finansial serangan siber, maka pertanyaan yang dibangun, yaitu: "Bagaimana dampak finansial perusahaan atas serangan siber?"

Identifikasi Penelitian Relevan

Kata kunci digunakan untuk memperoleh literatur yang relevan dengan topik penelitian.Istilah-istilah kunci pencarian yang berkaitan erat dengan fintech adalah: "cyberattack" DAN “financial impact.”

Table 1. Kriteria Inklusi

Kriteria	Inklusi	
Periode	2016-2023	Publikasi dalam 7 tahun
Bahasa	Inggris	Artikel yang diterbitkan dalam bahasa Inggris
Tipe Publikasi	Artikel Jurnal	Hanya artikel yang dipublikasikan di jurnal internasional bereputasi
Wilayah Geografis	Semua Negara	Temuan dari berbagai negara

Seleksi Artikel

Penelusuran artikel dilakukan melalui jurnal terindeks Sinta. Hasil penelusuran dengan menggunakan kata kunci pencarian ditemukan 200 artikel, yang diterbitkan oleh berbagai penerbit jurnal internasional bereputasi. Pencarian menggunakan aplikasi Publish or Perish dengan database google scholar. Artikel-artikel ini kemudian diperiksa untuk menentukan kesesuaiannya dengan pertanyaan penelitian. Artikel-artikel tersebut juga diperiksa untuk menemukan kemungkinan adanya duplikasi artikel dalam database yang berbeda. Pada tahap seleksi ini, tersisa 10 artikel yang sesuai dengan kriteria inklusi dan akan dilakukan analisis.

Memetakkan Data

Pada tahap pembuatan bagan data, artikel-artikel terpilih direduksi untuk meringkas data yang paling penting, data yang dicatat adalah data tentang penulis, tahun penelitian, lokasi penelitian, desain/metode, dan temuan. Artikel yang telah dikumpulkan selanjutnya akan dipilih artikel terfokus fintech yang membahas terkait dampak finansial perusahaan atas serangan siber. Pembahasan menyajikan temuan dari artikel terpilih disertaiketerbatasan dan peluang riset masa depan.

Mengumpulkan, Merangkum, dan Melaporkan Hasil

Tahap terakhir dari scoping review adalah menyusun, meringkas, dan melaporkan hasil penelitian, menyusun menghasilkan tabel yang berisi ekstraksi artikel yang dilakukan pada tahap pembuatan bagan data. Merangkum menghasilkan tema-tema atau pola utama dari temuan-temuan utama, dan melaporkan menghasilkan format laporan yang dalam hal ini untuk tujuan publikasi. Tabel 2 menunjukkan hasil dari penyusunan data.

Table 2. Data Collating

No.	Penulis	Tahun	Metode	Temuan
1	Sasha Romanosky	2016	Analisis Kritis	Dampak keuangan dari pelanggaran data pada perusahaan jauh lebih rendah daripada yang dirasakan umum, dengan sebagian besar perusahaan mengalami biaya kurang dari $200.000, bertentangan dengan jutaan yang sering dikutip dalam diskusi tentang insiden cyber
2	Shinichi Kamiya, Jun-Koo Kang, Jungmin Kim, Andreas Milidonis, René M. Stulz	2020	Pengembangan Model	Hasil ini menunjukkan bahwa serangan yang sukses dengan kehilangan informasi keuangan pribadi memberikan informasi negatif tentang risiko siber kepada target perusahaan, pemangku kepentingan mereka, dan pesaing mereka.
3	Onur Kemal Tosun	2021	Kuantitatif	Hasil utama menunjukkan bahwa imbal hasil harian yang berlebih menurun, volume perdagangan meningkat karena tekanan jual, dan likuiditas membaik setelah

				pengungkapan publik peristiwa peretasan perusahaan untuk pertama kalinya.
4	Olivér Gulyás & Gábor Kiss	2023	Analisis Tren	Serangan siber terhadap lembaga keuangan memiliki efek parah pada ekonomi global, dengan peningkatan vektor dan metode yang digunakan oleh penjahat dunia maya. Industri jasa keuangan adalah target utama, dengan meningkatnya ransomware dan serangan destruktif yang bertujuan untuk mengganggu layanan.
5	Niaz Kammoun, Ahmed Bounfour, Altay Özaygen & Rokhaya Dieye	2019	Studi Peristiwa	Hasil menunjukkan bahwa ada pengembalian abnormal negatif untuk NASDAQ setelah tanggal kecelakaan. Reaksi NASDAQ dan NYSE mirip, dan negatif untuk tanggal pertama kali diberitahukan tetapi positif setelah tanggal mulai kehilangan asli.
6	Maria Cristina Arcuri, Lorenzo Gai, Federica Ielasi and Elisabetta Ventisette	2020	Studi Peristiwa	menemukan bahwa pengembalian pasar negatif terjadi setelah pengumuman serangan siber yang dialami oleh perusahaan-perusahaan perhotelan. Investasi yang memadai dalam teknologi untuk keamanan siber dan pelatihan staf adalah relevan di sektor perhotelan untuk mengurangi risiko siber.
7	Nida Tariq	2018	Kaulitatif	Studi ini telah menyaksikan bahwa mungkin ada kasus serangan siber yang lebih sedikit pada institusi keuangan, tetapi dampaknya sangat parah dalam hal kerugian
				langsung dan tidak langsung. Juga telah terlihat bahwa serangan siber berkembang dengan cepat dibandingkan beberapa tahun yang lalu.
8	Daniel Castillo & Joseph Falzon	2018	Studi Peristiwa	Hasilnya jelas menunjukkan bahwa WannaCry memiliki efek positif pada pengembalian ekuitas perusahaan keamanan siber dan kendaraan investasi keamanan siber.
9	Marta Meisner	2018	Analisis Kritis	Hasil penelitian menunjukkan bahwa estimasi total biaya pelanggaran data digital bervariasi secara luas di antara berbagai laporan dan analisis. Alasan utama adalah penerapan berbagai metode estimasi dan kurangnya basis data yang lengkap dan dapat diandalkan akibat pengungkapan insiden siber yang tidak memadai.
10	Tweneboah-Koduah et al., 2018	2018	Kuantitatif	Hasil-hasil ini menyiratkan bahwa (1) mempelajari efek kumulatif dari serangan siber pada harga perusahaan yang terdaftar tanpa mengelompokkan mereka ke dalam berbagai sektor mungkin tidak memberikan informasi yang memadai, (2) perusahaan sektor keuangan cenderung bereaksi kumulatif terhadap serangan siber dalam periode 3 hari dibandingkan sektor lainnya, (3) perusahaan teknologi cenderung kurang reaktif terhadap pengumuman pelanggaran data; kemungkinan

				perusahaan semacam itu memiliki alat dan teknik yang diperlukan untuk menangani serangan siber skala besar.

HASIL

Berdasarkan pemetaan artikel, tema yang cenderung didiskusikan terdiri atas 1) Dampak Finansial dan Biaya Ekonomi Serangan Siber: (Romanosky (2016), Gulyas dan Kiss (2023), Tariq (2018), Meisner (2018) dan; 2) Reaksi Pasar Keuangan terhadap Serangan Siber: Kamiya et al. (2021), (Tosun, 2021), Kammoun et al. (2019), Arcuri et al. (2020), Tweneboah-Kodua et al. (2018) dan Castillo dan Falzon (2018).

Hasil kajian dari 10 artikel ilmiah menunjukkan bahwa serangan siber berdampak signifikan terhadap kondisi finansial perusahaan. Dampak tersebut tidak hanya bersifat langsung, seperti biaya pemulihan sistem dan litigasi hukum, tetapi juga mencakup kerugian tidak langsung seperti penurunan harga saham, kehilangan reputasi, gangguan operasional, dan berkurangnya kepercayaan investor serta konsumen (Meisner, 2018; Romanosky, 2016). (Romanosky, 2016), dalam studinya yang menganalisis lebih dari 12.000 peristiwa keamanan siber, menemukan bahwa meskipun terdapat persepsi publik bahwa serangan siber menyebabkan kerugian besar, kenyataannya kerugian finansial yang dialami perusahaan kerap kali relatif kecil dibandingkan yang dibayangkan. Namun, dampak ini sangat kontekstual dan tergantung pada jenis serangan dan kesiapan organisasi dalam merespons insiden.

Dampak serangan siber terhadap harga saham menjadi salah satu temuan dominan. Studi Kamiya et al. (2021) menunjukkan bahwa serangan yang melibatkan pencurian data keuangan pribadi memiliki dampak negatif signifikan terhadap harga saham perusahaan target. Temuan ini sejalan dengan studi Tosun (2021), yang menunjukkan adanya abnormal return negatif serta peningkatan volume transaksi akibat aksi jual oleh investor setelah pengungkapan publik serangan siber pertama kali terjadi. Bahkan, pasar modal seperti NASDAQ dan NYSE menunjukkan pola reaksi negatif terhadap pengumuman insiden, meskipun cenderung membaik setelah informasi tambahan tentang mitigasi muncul (Kammoun et al., 2019). Studi ini mendukung teori *efficient market hypothesis* yang menyatakan bahwa informasi negatif akan segera tercermin dalam harga pasar (Fama, 1970).

Selain itu, dampak finansial juga tampak berbeda antar sektor industri. Sektor keuangan menjadi salah satu yang paling rentan, dengan implikasi yang jauh lebih besar dibanding sektor lainnya. Gulyas dan Kiss (2023) serta Tariq (2018) menegaskan bahwa meskipun frekuensi serangan di sektor keuangan tidak selalu tinggi, namun dampaknya bisa sangat parah dalam hal kerugian langsung maupun gangguan sistemik terhadap perekonomian global. Tingkat ketergantungan pada infrastruktur digital serta tingginya nilai aset yang dikelola menjadikan lembaga keuangan sebagai sasaran empuk serangan dunia maya, terutama dalam bentuk ransomware dan serangan DDoS. Sementara itu, studi Arcuri et al. (2020) yang berfokus pada sektor perhotelan menemukan bahwa pengumuman serangan siber berdampak langsung pada pengembalian saham, menandakan tingginya sensitivitas investor terhadap risiko keamanan digital di industri layanan. Demikian pula dalam konteks kesehatan, Meisner (2018) menggarisbawahi bahwa pelanggaran data di rumah sakit dan institusi kesehatan dapat menyebabkan kerugian finansial yang besar, baik karena tuntutan hukum, biaya pemberitahuan, maupun penurunan kepercayaan publik terhadap penyedia layanan.

Studi juga menunjukkan bahwa karakteristik industri dan tingkat kesiapan keamanan digital memengaruhi tingkat kerentanan terhadap kerugian finansial. Tweneboah-Koduah et al. (2018) mencatat bahwa perusahaan teknologi cenderung lebih resilien terhadap pengumuman

serangan karena mereka memiliki perangkat dan prosedur pemulihan yang lebih baik. Sebaliknya, perusahaan sektor keuangan dan jasa lebih rentan terhadap dampak jangka pendek yang signifikan.

Namun demikian, tidak semua dampak serangan siber bersifat negatif. Studi oleh Castillo dan Falzon (2018) yang meneliti dampak serangan WannaCry menunjukkan bahwa peristiwa ini justru berdampak positif terhadap pengembalian saham perusahaan yang bergerak di bidang keamanan siber. Hal ini mencerminkan bahwa sektor tertentu dapat memperoleh manfaat ekonomi dari meningkatnya perhatian terhadap ancaman siber, terutama jika mereka menyediakan solusi mitigasi. Selain aspek finansial langsung, beberapa studi juga membahas pendekatan manajerial dan pengambilan keputusan yang perlu dilakukan untuk menghadapi risiko siber. Corallo et al. (2020) mengembangkan metodologi klasifikasi aset kritis di era Industri 4.0 untuk membantu manajemen dalam menilai tingkat risiko dan membuat keputusan investasi dalam keamanan digital.

Dari keseluruhan temuan, dapat disimpulkan bahwa serangan siber memiliki implikasi multidimensi terhadap kondisi keuangan perusahaan. Dampak ini sangat dipengaruhi oleh jenis industri, skala serangan, tingkat persiapan organisasi, serta bagaimana informasi serangan dikomunikasikan kepada publik. Sebagian besar studi memanfaatkan pendekatan *event study* dan analisis pasar saham untuk mengevaluasi dampak finansial, namun keterbatasan data dan praktik *under-reporting* masih menjadi tantangan besar dalam memperoleh estimasi kerugian yang akurat (Meisner, 2018; Romanosky, 2016).

PEMBAHASAN

Dampak Finansial dan Biaya Ekonomi Serangan Siber

Beberapa studi menekankan bahwa serangan siber menyebabkan beban finansial yang signifikan, baik dalam bentuk kerugian langsung seperti biaya investigasi, pemulihan sistem, dan pembayaran kompensasi, maupun kerugian tidak langsung seperti hilangnya pelanggan dan terganggunya operasi bisnis. Romanosky (2016) mencatat bahwa sebagian besar insiden siber sebenarnya tidak menghasilkan kerugian finansial sebesar yang dipersepsikan publik, tetapi tetap memunculkan tekanan terhadap perusahaan untuk meningkatkan keamanan. Hal ini diperkuat oleh Meisner (2018), yang menyoroti ketidakkonsistenan pelaporan biaya pelanggaran data dalam sektor kesehatan, sebagian karena kurangnya transparansi dan perbedaan metodologi estimasi.

Di sektor keuangan, Gulyas dan Kiss (2023) serta Tariq (2018) menegaskan bahwa meskipun jumlah serangan mungkin lebih sedikit dibanding sektor lain, dampaknya sangat parah, terutama karena tingginya nilai aset yang dikelola dan kepercayaan masyarakat yang menjadi landasan utama industri ini. Serangan terhadap bank dan lembaga keuangan juga memiliki potensi implikasi sistemik, yang dapat memengaruhi stabilitas ekonomi lebih luas. Kerugian tidak hanya bersifat monetisasi, tetapi juga reputasional, yang dalam jangka panjang bisa berdampak pada penurunan kepercayaan investor dan nasabah. Dari hasil klasifikasi ini, dapat disimpulkan bahwa meskipun besar kerugian bervariasi, kerugian finansial merupakan konsekuensi nyata dari serangan siber, yang memerlukan sistem pelaporan dan estimasi biaya yang lebih transparan dan komprehensif.

Reaksi Pasar Keuangan terhadap Serangan Siber

Sebagian besar artikel dalam kajian ini mengeksplorasi reaksi pasar saham sebagai indikator kuantitatif dampak finansial. Kamiya et al. (2021) menemukan bahwa serangan yang sukses dapat menurunkan harga saham secara signifikan, terutama jika informasi keuangan pribadi turut tercuri. Penurunan harga saham mencerminkan hilangnya kepercayaan pasar serta peningkatan persepsi risiko terhadap perusahaan.

Hal ini diperkuat oleh Tosun (2021) yang menunjukkan bahwa imbal hasil saham harian cenderung negatif pasca serangan, disertai peningkatan volume perdagangan akibat tekanan jual, serta peningkatan likuiditas yang bersifat sementara. Studi serupa oleh Kammoun et al. (2019) juga mendapati abnormal return negatif pada bursa NASDAQ dan NYSE, meskipun terjadi pemulihan setelah adanya klarifikasi atas insiden. Arcuri et al. (2020) menekankan bahwa sektor perhotelan secara khusus sangat terdampak, karena erat kaitannya dengan persepsi pelanggan dan keamanan data pribadi.

Menariknya, Tweneboah-Kodua et al. (2018) menunjukkan bahwa reaksi pasar bersifat sektoral: sektor keuangan lebih sensitif terhadap serangan dibanding sektor teknologi, yang cenderung lebih siap menghadapi insiden. Artinya, karakteristik industri dan kesiapan sistem keamanan turut menentukan tingkat kerentanan dan respons pasar.

SIMPULAN

Scoping review ini mengungkapkan bahwa serangan siber memiliki dampak finansial yang nyata dan multidimensi terhadap perusahaan. Dampak tersebut dapat berupa kerugian langsung seperti biaya pemulihan, kompensasi hukum, serta investigasi, maupun kerugian tidak langsung seperti menurunnya nilai saham, hilangnya reputasi, dan kepercayaan investor.

Reaksi pasar terhadap insiden siber cenderung negatif, terutama setelah pengumuman publik pertama, yang ditandai dengan penurunan harga saham dan meningkatnya tekanan jual. Sektor industri juga menunjukkan tingkat kerentanan yang berbeda-beda: sektor keuangan dan kesehatan cenderung mengalami dampak yang lebih besar, sementara perusahaan teknologi dan keamanan siber justru dapat mengalami penguatan nilai pasar, terutama jika dianggap mampu menawarkan solusi atas ancaman tersebut.

Selain itu, temuan menunjukkan bahwa kesiapan keamanan siber dan strategi manajemen risiko memegang peran penting dalam menekan besarnya kerugian finansial. Studi juga menekankan pentingnya perusahaan untuk mengklasifikasikan aset digital kritis dan mengintegrasikan keamanan siber ke dalam pengambilan keputusan strategis.

Penelitian ini memiliki beberapa keterbatasan yang perlu diperhatikan. Pertama, sebagian besar studi yang dianalisis bergantung pada data insiden yang dilaporkan secara publik, padahal banyak perusahaan tidak mengungkapkan informasi lengkap mengenai dampak keuangan dari serangan siber yang mereka alami. Hal ini menimbulkan keterbatasan dalam memperoleh gambaran utuh tentang kerugian aktual yang terjadi. Kedua, terdapat perbedaan metodologi estimasi kerugian dalam tiap studi, yang menyebabkan hasilnya tidak selalu dapat dibandingkan secara langsung atau digeneralisasi lintas kasus. Ketiga, sebagian besar literatur yang ditinjau berfokus pada konteks Amerika Serikat dan Eropa, sementara kajian di wilayah Asia Tenggara atau negara berkembang seperti Indonesia masih sangat minim. Keempat, mayoritas studi hanya mengkaji dampak finansial dalam jangka pendek, seperti reaksi pasar terhadap insiden yang baru diumumkan, sehingga potensi kerugian jangka panjang akibat serangan siber masih belum tergambarkan secara menyeluruh.

Berdasarkan keterbatasan tersebut, penelitian mendatang perlu diarahkan pada pengembangan model estimasi biaya yang lebih terstandar dan akuntabel agar memungkinkan perbandingan yang lebih valid antarstudi dan antarindustri. Selain itu, studi di negara berkembang seperti Indonesia penting untuk dilakukan, mengingat tingkat kesiapan keamanan digital dan literasi siber yang masih rendah. Penelitian longitudinal juga sangat dibutuhkan untuk menangkap dampak finansial jangka panjang dari serangan siber, termasuk perubahan strategi bisnis dan reputasi perusahaan pascainsiden. Di samping itu, penting pula untuk melakukan

kajian lintas sektor guna mengidentifikasi perbedaan karakteristik respons dan kerentanan masing-masing industri terhadap ancaman siber. Integrasi perspektif dari bidang akuntansi forensik, tata kelola perusahaan, dan manajemen risiko teknologi informasi juga dapat memperkaya pendekatan penelitian terhadap fenomena ini secara lebih holistik.

DAFTAR RUJUKAN

Arcuri, M. C., Gai, L., Ielasi, F., & Ventisette, E. (2020). Cyber attacks on hospitality sector: stock market reaction. *Journal of Hospitality and Tourism Technology*, *11*(2), 277–290. https://doi.org/10.1108/JHTT-05-2019-0080

Castillo, D., & Falzon, J. (2018). *An Analysis of the Impact of WannaCry Cyberattack on Cybersecurity Stock Returns*.

Corallo, A., Lazoi, M., & Lezzi, M. (2020). Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. In *Computers in Industry* (Vol. 114). Elsevier B.V. https://doi.org/10.1016/j.compind.2019.103165

Fonseca-Herrera, O. A., Rojas, A. E., & Florez, H. (2021). A Model of an Information Security Management System Based on NTC-ISO/IEC 27001 Standard. *IAENG International Journal of Computer Science*, *48*(2).

Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security*, *19*(1), 33–56. https://doi.org/10.3233/JCS-2009-0398

Gulyas, O., & Kiss, G. (2023). Impact of cyber-Attacks on the financial institutions. *Procedia Computer Science*, *219*, 84–90. https://doi.org/10.1016/j.procs.2023.01.267

Hossain, M. S., & Sultana, M. (2024). Digitalization of corporate finance and firm performance: global evidence and analysis. *Journal of Financial Economic Policy*. https://doi.org/10.1108/JFEP-04-2023-0109

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973–993. https://doi.org/10.1016/j.jcss.2014.02.005

Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, *139*(3), 719–749. https://doi.org/10.1016/j.jfineco.2019.05.019

Kammoun, N., Bounfour, A., Özaygen, A., & Dieye, R. (2019). Financial market reaction to cyberattacks. *Cogent Economics and Finance*, *7*(1). https://doi.org/10.1080/23322039.2019.1645584

Kitsing, M. (2017). Internet Banking as a Platform for E-Government. *Annual International Conference on Innovation and Entrepreneurship (IE 2017)*. https://doi.org/10.5176/2251-2039_IE17.30

Meisner, M. (2018). FINANCIAL CONSEQUENCES OF CYBER ATTACKS LEADING TO DATA BREACHES IN HEALTHCARE SECTOR. *Copernican Journal of Finance & Accounting*, *6*(3), 63. https://doi.org/10.12775/cjfa.2017.017

Pawar, S., & Palivela, D. H. (2022). LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs). *International*

Journal of Information Management Data Insights, *2*(1). https://doi.org/10.1016/j.jjimei.2022.100080

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, *2*(2), 121–135. https://doi.org/10.1093/cybsec/tyw001

Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). *Computers and Security*, *57*, 14–30. https://doi.org/10.1016/j.cose.2015.11.001

Sotamaa, O., Tyni, H., & Myöhänen, T. (2023). 'Even if the algorithm is a terrible workmate, you just need to learn to live with it': Perceptions of data analytics among game industry professionals. *European Journal of Cultural Studies*. https://doi.org/10.1177/13675494231168568

Tariq, N. (2018). Journal of Internet Banking and Commerce IMPACT OF CYBERATTACKS ON FINANCIAL INSTITUTIONS. In *Journal of Internet Banking and Commerce* (Vol. 23, Issue 2). http://www.icommercecentral.com

Thomas, G., & Sule, M.-J. (2023). A service lens on cybersecurity continuity and management for organizations' subsistence and growth. *Organizational Cybersecurity Journal: Practice, Process and People*, *3*(1), 18–40. https://doi.org/10.1108/ocj-09-2021-0025

Tosun, O. K. (2021). Cyber-attacks and stock market activity. *International Review of Financial Analysis*, *76*. https://doi.org/10.1016/j.irfa.2021.101795

Tweneboah-Kodua, S., Atsu, F., & Buchanan, W. (2018). Impact of cyberattacks on stock performance: a comparative study. *Information and Computer Security*, *26*(5), 637–652. https://doi.org/10.1108/ICS-05-2018-0060