MENGUKUR DAN MENGELOLA RISIKO *CYBERCRIME* DALAM *E-COMMERCE*: PERAN STRATEGIS *CYBERSECURITY* UNTUK KEAMANAN INFORMASI DAN PERLINDUNGAN DATA

Afzil Ramadian[1)], Amanda Fitriyani[2)], Neng Nanda Sarah Novita[3)]
[1]Fakultas Ekonomi dan Bisnis, Universitas Djuanda Bogor
E-mail: afzil.ramadian@unida.ac.id;
[2] Fakultas Ekonomi dan Bisnis, Universitas Djuanda Bogor
E-mail: amandafitriyani54351@gmail.com
[3] Fakultas Ekonomi dan Bisnis, Universitas Djuanda Bogor
E-Mail: Nandasrhnvt@gmail.com,

Abstract

Identifying and analyzing various types of cybercrime faced by e-commerce companies, measuring the level of cybercrime risk faced by e-commerce companies, and assessing the role of cyber security are the objectives of this research. The method used is a mathematical library review. The results show that measuring risk management, especially cybercrime risk in e-commerce, can be done by assessing the level of risk available and implementing risk management strategies. Regarding the important thing regarding the role and importance of cyber security in e-commerce, namely, cyber security protects valuable e-commerce assets, such as customer data, financial information, and intellectual property, from unauthorized access, theft, or damage. The conclusion is that cybercrime risk measurement, cybersecurity, and risk management are important elements to protect e-commerce businesses from cybercrime. The limitations of this research are limited to explaining the description and elaboration of the research results of several selected journal articles. However, it does not provide further analysis regarding the relationships between the articles discussed. It is hoped that further research will sharpen understanding and solutions to the challenges of cybercrime in e-commerce.

Keywords : *Cybercrime risk; Cybersecurity; Ecommerce*

1. PENDAHULUAN

Saat ini teknologi informasi sudah semakin berkembang dan menjadi sendi bagi kehidupan masyarakat sehingga tidak lagi sulit untuk ditemukan. Internet sudah menjadi kebutuhan bagi masyarakat ditandai dengan tingginya jumlah pengguna internet di Indonesia. Ketika penggunaan teknologi semakin matang, tentu berdampak pada kehidupan masyarakat sosial. Salah satu hal yang dilakukan pelaku ekonomi adalah penggunaan teknologi Internet dalam proses bisnisnya untuk melakukan transisi dari antarmuka ke Internet. Teknologi ini dikenal dengan sebutan perdagangan elektronik *(e-commerce*). Konsep transaksi *online* pada sebuah *e-commerce* merupakan langkah berkomunikasi antara produsen dan konsumen secara tidak langsung. Konsep tersebut banyak dimanfaatkan pembisnis pada perkembangan teknologi saat ini (Dewantara et al., 2023).

E-commerce adalah kependekan dari "*Electronic Commerce*" yaitu kegiatan melalui internet dalam melakukan pembelian dan penjualan produk. Transaksi bisnis pada sebuah *e-commerce* terjadi secara *online*, dengan konsumen dan produsen melakukan interaksi pada situs web, aplikasi seluler, maupun platform online lainnya (Lisnawati et al., 2023). Transaksi jual beli melalui *online* ini telah mengubah persepsi masyarakat ketika berbisnis. Kegiatan pembelian dan penjualan sebelumnya memerlukan pertemuan antara penjual dan pembeli, kini juga telah berubah. Kedua belah pihak baik itu konsumen dan produsen dapat melakukan pertemuan secara virtual hanya menggunakan media jual beli *online*. Tidak diperlukan lagi tatap muka secara langsung, cukup isi deskripsi produk di bidang yang ditentukan

pada aplikasi. Proses pembayaran melalui transfer digital dapat dilakukan kapan saja dan dimana saja (Abdi Baha & Popy Novita Pasaribu, 2023).

Tabel 1. Data Pengguna *E-Commerce* di Indonesia Tahun 2021-2023

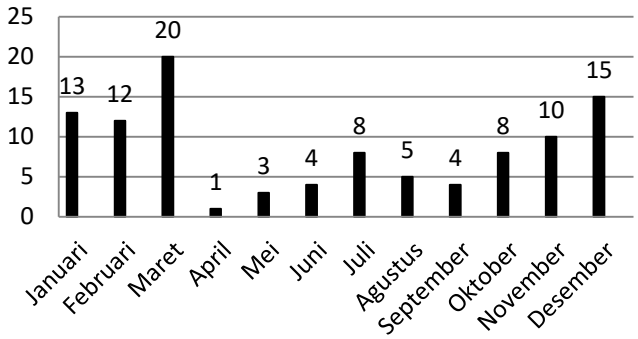
No	Tahun	Jumlah (Juta)
1	2021	158,65
2	2022	178,94
3	2023	196,47

Sumber : Statista Market Insights, 2024

Berdasarkan pada Tabel 1 tersebut, menunjukkan jumlah pengguna *e-commerce* di Indonesia di tahun 2023 adalah 196,47 juta mengalami kenaikan dibandingkan dengan tahun-tahun sebelumnya berjumlah 178,94 juta di tahun 2022 dan 158,65 juta di tahun 2021. *E-commerce* memiliki banyak keunggulan, antara lain akses yang mudah, alternatif produk beragam, medah dalam membandingkan harga, dan peningkatan efisiensi. Masalah keamanan informasi dan perlindungan data pribadi penting diperhatikan saat bertransaksi di *e-commerce* (Lisnawati et al., 2023). Informasi pribadi seperti nama, alamat, nomor telepon, dan informasi keuangan dapat dengan mudah dicuri atau disalahgunakan oleh pihak yang tidak bertanggung jawab. Ancaman terhadap keamanan data pribadi pengguna e-commerce beragam dan mencakup serangan *malware*, *phishing*, peretasan, dan pencurian identitas. Risiko yang timbul dari pelanggaran keamanan data pribadi tidak hanya dapat menyebabkan kerugian ekonomi bagi pengguna, tetapi juga merusak reputasi mereka di masyarakat (Kehista et al., 2023). Hal ini disebabkan oleh individu atau kelompok yang menyalahgunakan teknologi untuk melakukan kejahatan siber (*cybercrime*) yang dapat merugikan orang lain.

Kejahatan dunia maya adalah kejahatan yang dilakukan melalui Internet dengan menggunakan komputer dan jaringan teknologi yang disediakan oleh infrastruktur informasi dan komunikasi. Meningkatnya penggunaan teknologi *e-commerce* telah menyebabkan peningkatan kejahatan dunia maya di banyak negara. Aktivitas kriminal di internet terus membuat banyak orang khawatir akan risiko yang terkait dengan berbisnis di Internet. Oleh karena itu, agar perdagangan yang sukses di internet, langkah-langkah yang perlu digunakan dalam melindungi keamanan konsumen dan produsen. (Apau et al., 2019). Pendaftaran data pribadi dalam sistem elektronik menyebabkan peningkatan penggunaan sistem elektronik, termasuk perdagangan elektronik. Oleh karena itu, keamanan Internet menjadi semakin rentan dan dapat dengan mudah disusupi serta dieksploitasi oleh orang-orang jahat. Akibatnya, banyak kasus kebocoran data dapat terjadi (Irfan et al., 2023).

Gambar 1. Grafik Rekapitulasi Laporan Notifikasi Kebocoran Data 2023



Sumber : (BSSN, 2022)

Badan Siber dan Sandi Negara (BSSN) berhasil mengungkap 103 dugaan pelanggaran data. Pelanggaran data yang paling mencurigakan terjadi dengan 20 pelanggaran pada Maret 2023 dan 15 pelanggaran pada Desember 2023. Kejahatan dunia maya tidak hanya terjadi sekali. Kejadian cybercrime di Indonesia tercantum dalam temuan Direktorat Jenderal *Cybercrime* (Dittipidsiber) Bareskrim Polri yang menangani 4. 656 kejadian *cybercrime* sepanjang Januari hingga November 2020. Laporan penipuan online berada di urutan kedua dengan 1. 295 laporan. Hal ini bisa menjadi indikator penting kesadaran keamanan siber di Indonesia (Dewantara et al., 2023).

Berdasarkan tiga kriteria, tiga kriteria tersebut yaitu *platform* elektronik, pemilik, dan pengguna. Dapat diidentifikasikan bahwa pada industri *e-commerce* terdapat empat masalah keamanan utama yang kemungkinan dihadapi. Keempat topik keamanan tersebut adalah keamanan transaksi, perlindungan data, keamanan sistem perdagangan, dan kejahatan siber dalam perdagangan elektronik (*e-commerce*). Oleh karena itu, penting bagi pengguna e-niaga untuk memahami risiko keamanan terhadap informasi pribadi mereka dan mengambil tindakan yang tepat untuk melindungi informasi pribadi mereka. (Kehista et al., 2023). Konsumen dan pelaku ekonomi harus mampu melindungi diri dari ancaman tersebut melalui *cybersecurity*. Keamanan siber mengacu pada tindakan yang diambil untuk melindungi sistem komputer dari serangan digital dan akses tidak sah. Manajemen risiko dan penguatan keamanan siber memerlukan perhatian khusus. Manajemen risiko pada perusahaan *e-commerce* menjadi semakin penting untuk mengatasi tantangan dan ketidakpastian yang ada (Herdiana, 2018) dalam (Lisnawati et al., 2023). Pengukuran risiko kejahatan dunia maya, keamanan siber, dan manajemen risiko merupakan elemen kunci untuk melindungi perusahaan *e-commerce* dari kejahatan dunia maya. Memahami dan mengelola risiko kejahatan dunia maya membantu organisasi melindungi data dan reputasi mereka serta memastikan kelangsungan bisnis. Inilah yang menjadi fokus penelitian ini.

Studi ini tidak hanya berfokus pada ancaman dan risiko kejahatan siber, namun juga mengeksplorasi bagaimana manajemen risiko melalui pengukuran risiko membantu mengatasi tantangan kejahatan siber dan peran penting keamanan siber dalam manajemen risiko.

Penelitian sebelumnya oleh Muhammad Irfan dkk. (2023) Hasil jurnal berjudul "*Cybercrime Threat and the Role of Cybersecurity in E-Commerce: Systematic Literature Review*" menunjukkan bahwa mengatasi kejahatan *cyber di e-commerce* dapat menunjukkan bahwa institusi perlu bekerja sama dengan agen. Konsumen harus selalu waspada dan menghindari berbagi informasi pribadi dengan individu atau organisasi yang meragukan.

Novelty atau kebaruan dari penelitian ini terletak pada pendekatan yang holistik dan mendalam terhadap keterkaitan antara pengukuran risiko dalam manajemen risiko dengan tingginya pengguna *e-commerce* di Indonesia yang menimbulkan ancaman tingginya *cybercrime*. Penelitiaan ini menawarkan pendekatan terintegrasi yang mencakup manajemen risiko, pengukuran risiko, tingkat pengguna *e-commerce*, tingkat kejahatan *cybercrime*, dan peran *cybersecurity* dalam mengelola risiko *cybercrime*. Kebaruan juga dapat terletak pada kemampuannya untuk memberikan wawasan khusus dan solusi yang dapat diterapkan bagi pengguna teknologi internet khususnya pengguna e-commerce secara kontekstual dalam menghadapi risiko *cybercrime* demi keamanan informasi dan perlindungan data.

Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis berbagai jenis ancaman kejahatan dunia maya (*cybercrime*) yang dihadapi oleh perusahaan *e-commerce*, mengukur tingkat risiko kejahatan dunia maya (*cybercrime*) yang dihadapi oleh perusahaan *e-commerce*, dan menilai peran keamanan siber (*cybersecurity*). Secara keseluruhan, penelitian ini bertujuan untuk meningkatkan pemahaman tentang risiko kejahatan dunia maya (*cybercrime*) di *e-commerce* dan membantu perusahaan e-commerce meningkatkan keamanannya. Penelitian ini diharapkan dapat memberikan kontribusi berharga pada literatur tentang keamanan e-commerce dan membantu perusahaan *e-commerce* melindungi diri dari kejahatan dunia maya (*cybercrime*).

2. METODE PENELITIAN

Metode yang digunakan adalah tinjauan pustaka matematis (Irfan et al., 2023). Langkah pertama adalah menentukan tujuan dan hasil yang diinginkan dari penelitian yang akan dilakukan. Penelitian ini dilakukan untuk lebih memahami risiko kejahatan dunia maya di *e-commerce* dan membantu perusahaan e-commerce meningkatkan keamanannya. Untuk mencapai tujuan tersebut, dapat dirumuskan pertanyaan penelitian sebagai berikut: (1) Bentuk kejahatan dunia maya apa yang mengancam e-commerce? (2) Apa peran keamanan siber e-commerce dalam memprediksi risiko kejahatan dunia maya? Langkah kedua adalah penelitian Mencari makalah yang berkaitan dengan suatu tema. Pencarian artikel dilakukan di *Google Scholar* dengan menggunakan kata kunci "*cybercrime, cybersecurity, e-commerce risk"*. Langkah ketiga adalah memilih item yang diidentifikasi sebelumnya dalam proses pencarian. Setelah proses pemilihan item dilakukan, berbagai item diambil dan disimpan di Mendeley untuk mengatur item yang dipilih. Pada langkah terakhir, penulis melakukan analisis terhadap makalah yang dipilih berdasarkan pertanyaan penelitian dan mengidentifikasi bentuk risiko kejahatan siber yang mengancam perdagangan elektronik dan pentingnya keamanan siber dalam melindungi dari ancaman kejahatan siber, keamanan informasi, dan data Anda saat ini mempunyai gambaran komprehensif tentang peran tersebut. Perlindungan.

Instrumen

Pencarian artikel di *Google Scholar* dengan kata kunci risiko kejahatan dunia maya, keamanan siber, dan perdagangan elektronik" menghasilkan 471 artikel. Berdasarkan hasil yang diperoleh, kami memilih makalah dan menggunakannya dalam penelitian ini. Berikut rincian proses seleksi artikel jurnal :

1. Makalah diterbitkan dalam jangka waktu 5 tahun, yaitu dari tahun 2020 hingga 2024. Total artikel yang diterima sebanyak 363 artikel.
2. Artikel yang dapat menjawab pertanyaan penelitian yang telah dirumuskan sebelumnya. Kami memilih artikel yang dapat menjawab pertanyaan penelitian ini, sehingga menghasilkan 10 artikel dengan kualitas terbaik untuk setiap pertanyaan penelitian.
   Kata kunci yang dimasukkan dan jumlah artikel adalah sebagai berikut.
   a. Risiko Ancaman *Cybercrime* dalam Perdagangan Elektronik (*Cybercrime Threats in Electronic Commerce*) Maksimal 5 artikel.
   b. Peran Keamanan Siber dalam Perdagangan Elektronik (*The Role of Cybersecurity in Electronic Commerce*) mempunyai 5 artikel

Berdasarkan tingkat pemilihan item di atas, terlihat bahwa jumlah jurnal yang memenuhi kriteria yang ditentukan adalah 10 jurnal. Artikel yang diidentifikasi dapat dikategorikan menurut tahun publikasi, metode penelitian, dan topik yang dibahas. Setelah mengelompokkan artikel yang digunakan dalam penelitian ini berdasarkan tahun terbit dari tahun 2020 hingga 2024, tahun 2023 memiliki jumlah terbitan terbanyak yaitu sebanyak lima artikel. Sebaliknya, jumlah artikel yang diterbitkan paling sedikit terjadi pada tahun 2024, yakni sebanyak 0 artikel yang diterbitkan. Pada tahun 2020 hingga 2024, publikasi artikel mengenai risiko ancaman kejahatan siber dan peran keamanan siber dalam e-commerce sangat fluktuatif dan cenderung meningkat. Hasil pengklasifikasian artikel berdasarkan tahun penerbitan ditunjukkan pada Tabel 2 di bawah ini.

Tabel 2. Klasifikasi Artikel Berdasarkan Tahun Terbit

No	Tahun	Jumlah Artikel
1	2020	1
2	2021	2
3	2022	2
4	2023	5
5	2024	0
Jumlah		10

Klasifikasi makalah berikut yang digunakan dalam penelitian ini didasarkan pada metode penelitian yang diidentifikasi. Metode yang paling banyak digunakan adalah metode kualitatif dan tinjauan literatur dengan empat artikel. Metode pendekatan kualitatif dan tinjauan pustaka didasarkan pada informasi non-numerik seperti teks dan foto, sedangkan penyaringan statistik menggunakan fakta-fakta sekunder yang diperoleh secara tidak langsung dan analisis data yang diperoleh dari buku dan surat kabar untuk meningkatkan kualitas literatur. majalah, fakta statistik atau internet (Sudarmadi & Runturambi, 2019) dalam (Indah & Sidabutar, 2022). Hasil pengklasifikasian artikel berdasarkan metode penelitian ditunjukkan pada Tabel 3 di bawah ini:

Tabel 3. Klasifikasi Artikel Berdasarkan Metode Penelitian

No	Metode Penelitian	Jumlah Artikel
1	Studi Literatur	3
2	Analisis kuantitatif dengan skala likert	1
3	Kualitatif dan Kajian Pustaka	4
4	Pendekatan perundang-undangan (Statute Approach) dan Pendekatan Konseptual (Conceptual Approach)	1
5	Pengabdian masyarakat	1
Jumlah		10

Terakhir, pengklasifikasian artikel berdasarkan topik yang dibahas. Menunjukkan bahwa topik yang dibahas dalam artikel-artikel tersebut secara umum adalah risiko kejahatan siber di *e-commerce* dan keamanan siber sebagai antisipasi tindakan tersebut. Hasil pengklasifikasian artikel menurut topik pembahasan disajikan pada Tabel 4 berikut ini:

Tabel 4. Klasifikasi Artikel Berdasarkan Topik Pembahasan

No	Judul	Penulis
1	Ancaman Cybercrime Dan Peran Cybersecurity Pada E-Commerce: Systematic Literature Review	(Irfan et al., 2023)
2	Manajemen Insiden Keamanan Cyber Security Pemerintahan Indonesia Agar Terciptanya	(Dewantara et al., 2023)

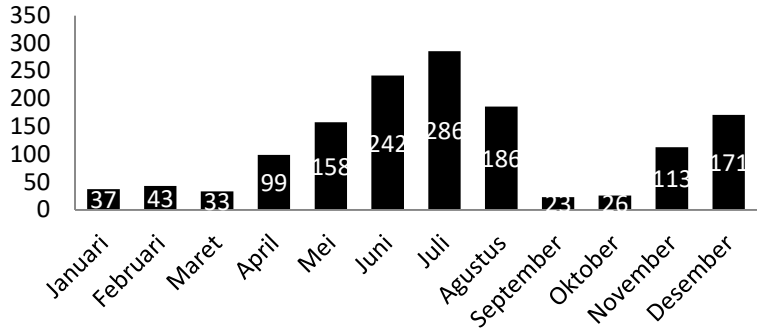
	Keamanan Transaksi E-Commerce Di Indonesia	
3	Peran Cyber Security Terhadap Keamanan Data Penduduk Negara Indonesia (Studi Kasus: Hacker Bjorka)	(Indah & Sidabutar, 2022)
4	Strategi Indonesia Membentuk Cyber Security Dalam Menghadapi Ancaman Cyber Crime Melalui Badan Siber Dan Sandi Negara	(Ginanjar, 2022)
5	Mengukur Keamanan Siber Indonesia Melalui Indikator Pilar Kerjasama Dalam Global Cybersecurity Index (Gci)	(Cloramidine & Badaruddin, 2023)
6	Tranformasi Digital Dan Ancaman Cybercrime	(Rolando et al., 2023)
7	Cybercrime Dan Dampaknya Pada Teknologi E-Commerce	(Rahayu et al., 2021)
8	Analisis Keamanan Data Pribadi pada Pengguna E-Commerce: Ancaman, Risiko, Strategi Kemanan (Literature Review)	(Kehista et al., 2023)
9	Pelanggaran Data Dan Pencurian Identitas Pada E-Commerce	(Nafi'ah, 2020)
10	Cybercrime dan Cybersecurity pada Fintech: Sebuah Tinjauan Pustaka Sistematis	(Riskiyadi et al., 2021)

3. HASIL DAN PEMBAHASAN

Electronic commerce (E-commerce) adalah aktivitas yang melibatkan transaksi jual beli oleh produsen dan konsumen dengan pemanfaatan teknologi digital yang diimplementasikan dalam kegiatan usaha melalui penggunaan internet (Maulana et al., 2015). Tingginya akses pengguna online atau internet menjadi salah satu faktor semakin maraknya kasus ancaman *cyber*. Perkembangan teknologi secara tidak langsung mempengaruhi kemudahan penyebaran informasi dan data. Hal ini dapat meningkatkan risiko kejahatan dunia maya. Penanggulangan kejahatan dunia maya ini berdampak negatif, menyebabkan kerugian yang signifikan tidak hanya bagi perusahaan tetapi juga bagi pelanggannya. Hilangnya kepercayaan pengecer dan pelanggan terhadap belanja online dianggap sebagai biaya yang tidak terlihat akibat kejahatan dunia maya (Irfan et al., 2023).

Tim Pusat Kontak Siber BSSN selama tahun 2023 mendapatkan informasi sekitar 1.417 pengaduan *cyber*. Aduan dengan jumlah tertinggi terjadi pada bulan Juli dengan total 286 aduan, dapat dilihat pada grafik di bawah ini.

Gambar 2. Rekapitulasi Aduan *Cyber* 2023



Sumber : (BSSN, 2022)

Berdasarkan studi kasus pada penelitian yang dilakukan oleh Rizkya Amalia Putri (2022) ditemukan sebuah permasalahan terkait terdapat kebocoran data phonebook dimana salah satu konsumen Shopee bernama Liana Therandhana menceritakan kronologi kebocoran datanya. Pada tanggal 10 juli 2019 pukul 21.00 WIB Liana Therandhana membuka aplikasi shopee dan langsung tertuju pada notifikasi yang masuk di akun miliknya ternyata terdapat keterangan notifikasi muncul semua data dari phonebook. Keterangan notifikasi tersebut bahkan lebih dari satu dan malam itu juga Liana sendiri langsung mengirim email kepada pihak Shopee untuk menanyakan perihal tersebut. Karena Liana takut bila *phonebook* dipakai oleh oknum yang tidak bertanggung jawab secara tidak langsung oknum yang telah mencuri data privasi *phonebook* dan bias saja untuk melakukan modus atau aksi kejahatan lainnya. Dengan demikian, dari adanya kasus tersebut pihak shopee melakukan upaya preventif dalam menyelesaikan permasalahan kebocoran data pribadi phonebook. Dalam menyelesaikan permasalahan kebocoran data pribadi yang ada di dalam perdagangan elektronik, Shopee membentuk tim untuk memitigasi risiko yang terdiri dari sub- unit yakni tim *data analytics* dan *data science, analytics regional, dan tim software engineering and technology*. Selain itu, pertanggungjawaban pihak Shopee terhadap kebocoran data pribadi didasari oleh peraturan yang tertera di UU Informasi dan Transaksi Elektronik yaitu digunakan cara melaksanakan semua upaya-upaya demi melindungi sistem elektronik demi menerapkan risiko manajemen sesuai dengan kaidah-kaidah yang disahkan (Putri, 2022).

Tentunya dalam hal ini dapat dijadikan sebuah pernyataan mengenai asumsi sebagian besar masyarakat yang mengkhawatirkanan ketika menggunakan aplikasi *e-commerce*. Dengan demikian, kejadian tersebut memperlihatkan bagaimana faktor keamanan terkait privasi data pengguna cukup rentan terhadap ancaman *cybercrime*. Menghadapi ketidakpastian dan tantangan yang ada maka dalam hal ini manajemen risiko pada sebuah bisnis *e-commerce* menjadi semakin penting. Risiko yang berkaitan pada *e-commerce* yaitu keamanan privasi, penipuan, aturan tidak sesuai, identitas yang hilang, rentannya serangan *cyber*, serta kelangsungan bisnis yang dipengaruhi oleh ulasan negatif. Manajemen risiko pada sebuah bisnis *e-commerce* yaitu meliputi identifikasi, pengukuran, dan pengelolaan risiko yang berhubungan dengan operasional bisnis tersebut. Manajemen risiko bertujuan untuk meminimalisir dampak negatif dan memanfaatkan peluang yang befsifat positif pada sebuah lingkungan bisnis yang dinamis dan kompelks (Herdiana, 2018).

Pengukuran manajemen risiko khususnya risiko *cybercrime* pada *e-commerce* itu dapat dilakukan melalui penilaian akan tingkat risiko yang tersedia serta mengimplementasikan

strategi pengelolaan risiko. Adapun strategi pendekatan pada umumnya dilakukan dalam pengukuran manajemen risiko pada sebuah *e-commerce* (Kurniandy, 2016), yaitu sebagai berikut:

1) Analisis Probabilitas-Dampak: Probabilitas dapat dinyatakan dalam persentase atau skala numerik lain yang menunjukkan kemungkinan terjadinya suatu risiko. Dampaknya dapat mencakup kerugian finansial, reputasi, atau operasional. Menggabungkan probabilitas dan dampak memberikan pemahaman yang dapat diandalkan tentang tingkat risiko secara keseluruhan.
2) Analisis Sensitivitas: Mengidentifikasi dan menganalisis faktor-faktor penting yang berkontribusi terhadap risiko bagi perusahaan *e-commerce*.
3) Metrik Kinerja : Metrik kinerja dapat mencakup jumlah insiden penipuan yang terdeteksi, waktu pemulihan dari serangan siber, tingkat kepatuhan terhadap peraturan, atau tingkat keberhasilan penerapan kebijakan keamanan. Dengan menggunakan metrik yang jelas, perusahaan dapat mengukur kemajuan manajemen risiko mereka dan menilai efektivitas strategi yang diterapkan.
4) Evaluasi Keuangan: Keuangan: Mengevaluasi dampak risiko terhadap kinerja keuangan perusahaan, antara lain: Contoh: hilangnya pendapatan, biaya pemulihan setelah serangan siber, kerugian akibat penipuan, dll. Penilaian ini membantu dalam memahami kontribusi risiko terhadap hasil keuangan perusahaan dan mendorong keputusan manajemen risiko yang cerdas.
5) Audit dan Evaluasi Eksternal: Pihak ketiga yang independen dapat dilibatkan untuk mengevaluasi kebijakan, prosedur, dan sistem manajemen risiko yang ada. Hasil audit atau penilaian eksternal ini memberikan gambaran obyektif mengenai efektivitas manajemen risiko pada perusahaan *e-commerce*.

Strategi pendekatan umumnya dapat digunakan untuk pengukuran risiko pada sebuah *e-commerce*. Strategi tersebut bervariasi tergantung kriteria, spesifikasi, ciri bisnis dan restrukturisasi organisasi. Pengukuran risiko *cybercrime* pada *e-commerce* merupakan proses yang dilakukan untuk mengidentifikasi, menganalisis, serta mengevaluasi potensi dari kerugian finansial dan reputasi yang dapat ditimbulkan oleh serangan *cyber*. Tujuannya yaitu untuk memahami tingkat risiko yang dihadapi bisnis dan mengambil langkah-langkah yang tepat untuk menguranginya.

Cybersecurity (keamanan siber) didefinisakan sebagai suatu proses yang dijalankan untuk mempertahankan dan mengurangi masalah privasi, keintegritasan serta terhadap adanya fakta yang tersedia. Proses tersebut dapat menjaga sistem informasi dari segala serangan fisik dan serangan *cyber* (Indah & Sidabutar, 2022). *Cybersecurity* merujuk pada perlindungan terhadap informasi sesuai dengan jenis dan kepekaaan informasi yang ada dalam suatu organisasi untuk penggunaanya secara strategis (Horne et al., 2016) dalam (Irfan et al., 2023). *Cybersecurity* dikatakan memegang peran cukup penting dalam melindungi bisnis *e-commerce* dari berbagai ancaman *cybercrime* yang semakin marak dan canggih. Beberapa hal penting mengenai peran dan pentingnya *cybersecurity* dalam *e-commerce* yaitu, *cybersecurity* melindungi aset berharga *e-commerce*, seperti data pelanggan, informasi keuangan, dan kekayaan intelektual, dari akses tidak sah, pencurian, atau kerusakan. *Cybersecurity* adalah sebagai perlindungan terhadap struktur *cyber* dari munculnya ancaman *cyber*. Oleh karena itu, *cybersecurity* bermanfaat cukup signifikan ketika melakukan perlindungan keamanan informasi maupun data dikarenakan perlu supaya melindungi informasi serta memberikan jaminan bahwa data yang dikirim dalam kondisi aman.

4. KESIMPULAN

Manajemen risiko pada sebuah *e-commerce* menjadi semakin penting dalam mengelola risiko-risiko terkait *e-commerce*. Strategi pendekatan dapat dilakukan dalam pengukuran tingkat risiko pada *e-commerce*, strategi tersebut bervariasi tergantung kriteria, spesifikasi, ciri bisnis dan restrukturisasi organisasi. Merujuk pada *e-commerce*, *cybersecurity* mempunyai peran penting dalam melindungi data yang terkandung didalamnya. Pengukuran risiko *cybercrime*, *cybersecurity*, dan manajemen risiko adalah elemen penting untuk melindungi *e-commerce* dari ancaman *cybercrime*. Dengan memahami dan mengelola risiko *cybercrime*, bisnis dapat melindungi data dan reputasi mereka, serta memastikan kelangsungan operasi mereka. Keterbatasan dalam penelitian ini sebatas menjelaskan gambaran dan elaborasi hasil penelitian beberapa artikel jurnal yang dipilih. Akan tetapi, tidak memberikan analisis lebih lanjut mengenai hubungan antar artikel yang dibahas. Bagi penelitian selanjutnya diharapkan lebih mempertajam pemahaman dan solusi terhadap tantangan *cybercrime* dalam *e-commerce*.

5. UCAPAN TERIMA KASIH

Penulis ingin mengucapkan banyak terima kasih kepada semua pihak yang telah membantu penyusunan jurnal penelitian ini. Pencapaian ini tidak akan terjadi tanpa dukungan Anda semua.

Penulis ingin mengucapkan terima kasih kepada referensi studi literatur beserta penelitian terdahulu yang telah dilakukan sebelumnya, juga terhadap para pakar ahli yang menambah pengetahuan dan sebagai referensi bagi penulis menyusun dan menganalisis jurnal penelitian ini.

Penulis ingin sekali lagi mengucapkan terima kasih kepada semua orang yang telah memberikan bantuan berupa masukan dan saran. Untuk mencapai lebih banyak pencapaian penting di masa depan, mari kita terus belajar dan memperbaiki setiap kekurangan untuk masa depan yang lebih baik

DAFTAR PUSTAKA

Abdi Baha, M., & Popy Novita Pasaribu. (2023). Tipe Konsumen Marketplace Blibli.Com Menurut Teori Hausel. *Jurnal Visionida*, *9*(2), 139–153. https://doi.org/10.30997/jvs.v9i2.9472

Apau, R., Koranteng, F. N., & Gyamfi, S. A. (2019). Cyber-Crime and its Effects on E-Commerce Technologies. *Journal of Information*. https://doi.org/10.18488/journal.104.2019.51.39.59

BSSN. (2022). Lanskap Keamanan Siber Indonesia 2022. *Badan Siber Dan Sandi Negara*, *70*.

Cloramidine, F., & Badaruddin, M. (2023). Mengukur Keamanan Siber Indonesia Melalui Indikator Pilar Kerjasama Dalam Global Cybersecurity Index (GCI). *Populis : Jurnal Sosial Dan Humaniora*, *8*(1), 57–73. https://doi.org/10.47313/pjsh.v8i1.1957

Dewantara, R., Salsabila, N. G., & Asiska, W. A. (2023). Manajemen Insiden Keamanan Cyber Security Pemerintahan Indonesia Agar Terciptanya Keamanan Transaksi E-Commerce

Di Indonesia. *Jurnal ABDIMAS-IBISA Pengabdian Kepada Masyarakat*, *1*(2), 34–41.

Ginanjar, Y. (2022). Strategi Indonesia Membentuk Cyber Security Dalam Menghadapi Ancaman Cyber Crime Melalui Badan Siber Dan Sandi Negara. *Jurnal Dinamika Global*, *7*(02), 291–312. https://doi.org/10.36859/jdg.v7i02.1187

Herdiana, Y. (2018). Manajemen Resiko Keamanan E-Commerce. *Tematik*. https://doi.org/10.38204/tematik.v5i1.145

Indah, F., & Sidabutar, A. Q. (2022). Peran Cyber Security Terhadap Keamanan Data Penduduk Negara Indonesia (Studi Kasus: Hacker Bjorka). *Jurnal Bidang Penelitian Informatika*, *1*(1), 2. https://ejournal.kreatifcemerlang.id/index.php/jbpi/article/view/78%0Ahttps://ejournal.kreatifcemerlang.id/index.php/jbpi/article/download/78/8

Irfan, M., Elvia, M., & Dania, S. (2023). Ancaman Cybercrime dan Peran Cybersecurity pada E-commerce: Systematic Literature Review. *Jursima*, *11*(1), 110–121.

Kehista, A. P., Fauzi, A., Tamara, A., Putri, I., Fauziah, N. A., Klarissa, S., & Damayanti, V. B. (2023). Analisis Keamanan Data Pribadi pada Pengguna E-Commerce: Ancaman, Risiko, Strategi Kemanan (Literature Review). *Jurnal Ilmu Manajemen Terapan*, *4*(5), 625–632. https://dinastirev.org/JIMT/article/view/1541

Kurniandy, W. (2016). Analisis Manajemen Risiko Sistem Pembayaran Transaksi Online Pada Toko Online Mataharimall.Com. In *Psychology Applied to Work: An Introduction to Industrial and Organizational Psychology, Tenth Edition Paul*.

Lisnawati, T., Hussaen, S., & Nuridah, S. (2023). Manajemen Risiko dalam Bisnis E-commerce : Mengidentifikasi ,. *Jurnal Pendidikan …*, *7*, 8252–8259. https://repository.bsi.ac.id/repo/files/372665/download/11.-Publikasi-Jurnal.pdf

Maulana, S. M., Susilo, H., & Riyadi. (2015). Implementasi E-Commerce Sebagai Media Penjualan Online. *Jurnal Administrasi Bisnis*.

Nafi'ah, R. (2020). Pelanggaran Data Dan Pencurian Identitas Pada E-Commerce. *Cyber Security Dan Forensik Digital*, *3*(1), 7–13. https://doi.org/10.14421/csecurity.2020.3.1.1980

Putri, R. A. (2022). Penyelesaian Sengketa Kebocoran Data Pribadi Phonebook dalam E-Commerce. *Skripsi*.

Rahayu, S. K., Ruqoyah, S., Berliana, S., Pratiwi, S. B., & Saputra, H. (2021). Cybercrime dan dampaknya pada teknologi e-commerce. *Journal of Information System, Applied, Management, Accounting and Research*, *5*(3), 632. https://doi.org/10.52362/jisamar.v5i3.478

Riskiyadi, M., Anggono, A., & Tarjo. (2021). Cybercrime dan Cybersecurity pada Fintech:

Sebuah Tinjauan Pustaka Sistematis. *Jurnal Manajemen Dan Organisasi*, *12*(3), 239–251. https://doi.org/10.29244/jmo.v12i3.33528

Rolando, D. M., Aulia, H. H., Rahmaningsih, A. A., & Andani, M. T. (2023). Transformasi Digital dan Ancaman Cybercrime. *Siyasah: Jurnal Hukum Tata Negara*, *3*(1), 68–84.