JURSIMA
Jurnal Sistem Informasi & Manajemen
ISSN : 2338-1523, E-ISSN: 2541- 576X

ANCAMAN *CYBERCRIME* DAN PERAN *CYBERSECURITY* PADA *E-COMMERCE*: *SYSTEMATIC LITERATURE REVIEW*

Muhammad Irfan[1)], Mairisa Elvia[2)], Shaquila Dania[3)]
[1,2,3)] Program Studi Magister Akuntansi, Universitas Andalas, Kota Padang
email: 1910531006_muhammad@student.unand.ac.id

ABSTRAK

Penelitian ini bertujuan untuk mengetahui tantangan *cybercrime* yang dihadapi oleh *e-commerce* serta tindakan antisipasi berupa *cybersecurity* untuk menanggulangi tantangan tersebut. Penelitian ini menggunakan metode tinjauan pustaka matematis atau *systematic literature review* (SLR). Hasil menunjukkan penanganan kejahatan siber pada *e-commerce* harus dilakukan secara kolektif oleh pelanggan, perusahaan *e-commerce*, dan penegak hukum. Konsumen harus selalu waspada dan memastikan bahwa mereka tidak menyediakan informasi pribadi kepada orang atau organisasi yang tidak dapat dipercaya. Keterbatasan penelitian ini sebatas memberikan gambaran dan elaborasi dari hasil penelitian dari masing-masing artikel yang dipilih, namun tidak memberikan analisis lanjutan mengenai keterkaitan antar artikel yang dibahas. Rekomendasi penelitian selanjutnya dapat menambah ruang lingkup artikel yang diteliti.

Kata Kunci: *Cybercrime, Cybersecurity, E-commerce*

ABSTRACT

This study aims to determine the cybercrime challenges faced by e-commerce as well as anticipatory actions in the form of cybersecurity to overcome these challenges. This study used a systematic literature review (SLR) method. The results show that the handling of cyber crimes in e-commerce must be carried out collectively by customers e-commerce companies, and law enforcement. Consumers should always be vigilant and ensure that they do not provide personal information to people or organizations they cannot trust. The limitations of this study are limited to providing an overview and elaboration of the research results from each of the selected articles, but does not provide further analysis regarding the interrelationships between the articles discussed. Recommendations for further research can add to the scope of the article under study.

Keywords: *Cybercrime, Cybersecurity, E-commerce*

PENDAHULUAN

Menurut Nafi'ah (2020), teknologi mencakup semua sarana yang digunakan untuk menyediakan kebutuhan dan kenyamanan hidup manusia. Teknologi informasi sediri, memilki manfaat positif yang dapat diperoleh oleh setiap orang, baik individu atau kelompok yang melakukan suatu aktivitas (Anggono *et al.*, 2021). Belanja online, juga dikenal sebagai "*e-commerce*", adalah salah satu inovasi yang muncul di masyarakat yang mengikuti tren ini. *E-commerce* adalah tempat di mana produsen dan konsumen, atau penjual dan pembeli, berkumpul untuk melakukan transaksi secara online melalui jaringan internet.

Teknologi *e-commerce* adalah mekanisme bisnis yang bekerja secara elektronik dengan berfokus pada transaksi bisnis online dan memiliki peluang untuk membangun hubungan dengan konsumen (Rabiah *et al.*, 2020). Bisnis ini bisa berjalan selama 24 jam sehari, 7 hari seminggu, dan luas pasarnya menjangkau dari tingkat lokal hingga mancanegara.

JURSIMA
Jurnal Sistem Informasi & Manajemen
ISSN : 2338-1523, E-ISSN: 2541- 576X

Dengan *e-commerce* memungkinkan pelanggan bertransaksi dengan cepat dan biaya yang murah tanpa melalui proses yang berbelit-belit, di mana pihak pembeli cukup mengakses internet ke website perusahaan yang mengiklankan produknya di internet, yang kemudian pihak pembeli cukup mempelajari *term of condition* (ketentuan-ketentuan yang disyaratkan) pihak penjual (Wajong dan Putri, 2010).

Bisnis berbasis internet juga memiliki beberapa keuntungan, seperti peningkatan efisiensi perusahaan, pemasaran produk yang lebih luas, dan tidak ada batasan waktu atau ruang (Wajong dan Putri, 2010). Namun, meskipun bisnis online memiliki beberapa manfaat, juga ada efek negatifnya. Ini disebabkan oleh penyalahgunaan teknologi oleh individu atau kelompok untuk melakukan kejahatan dunia maya, juga dikenal sebagai *Cybercrime*, yang dapat membahayakan orang lain (Anggono *et al.*, 2021).

Kejahatan dunia maya semakin meningkat di banyak negara karena penggunaan teknologi *e-commerce* yang meningkat (Apau *et al.*, 2019). Karena aktivitas kejahatan internet, bahaya yang terkait dengan menjalankan bisnis melalui Internet terus menjadi sumber kekhawatiran bagi banyak orang. Oleh karena itu, tindakan harus diambil untuk menjaga keamanan pelanggan dan bisnis agar transaksi bisnis melalui Internet dapat berhasil (Apau *et al.*, 2019).

Cybercrime adalah pelanggaran yang dilakukan di internet dengan menggunakan komputer dan jaringan teknologi yang disediakan oleh infrastruktur Informasi dan Komunikasi (Fahlevi *et al.*, 2019). Tingkat kepercayaan yang rendah terhadap aplikasi *e-commerce* adalah masalah utama yang dihadapi pengguna. Keamanan data kini menjadi masalah utama dalam manajemen dan pemeliharaan data bisnis (Putri *et al.*, 2020).

Pendaftaran data pribadi ke dalam sistem elektronik menyebabkan peningkatan penggunaan sistem elektronik apapun, termasuk *e-commerce*. Oleh karena itu, keamanan internet menjadi semakin rentan dan mudah dibobol dan disalahgunakan oleh individu jahat. Akibatnya, banyak kasus kebocoran data yang terjadi. Misalnya, dalam kebocoran data yang terjadi pada bulan Mei 2020 kemarin, sepuluh perusahaan digital mengalami kebocoran data dengan total 73 juta lebih data bocor, termasuk situs *e-commerce* Bhinneka.com, yang memiliki 1,2 juta pelanggan. Sekelompok hacker menjual data pribadi pelanggan tersebut secara bebas di pasar web gelap, dengan tujuan untuk mendapatkan keuntungan dari penjualan data tersebut (Firmansyah Putri dan Fahrozi, 2021)

Kasus *cybercrime* tidak cukup satu kali saja yang pernah terjadi. Jumlah kasus *cybercrime* di Indonesia dapat dibuktikan oleh 4.586 laporan yang diterima oleh Direktorat Tindak Pidana Siber Bareskrim Polri dari Januari hingga Desember 2019. Dengan 1.617 kasus, laporan tentang penipuan online nomor dua. Kebanyakan korban *cybercrime* adalah pengguna atau pelaku *e-commerce*, yaitu pembeli dan penjual. Dengan demikian, ini dapat dianggap sebagai catatan penting tentang tingkat kesadaran masyarakat Indonesia tentang keamanan siber (Rahmadi dan Rafie, 2020).

Untuk meningkatkan pemahaman akademisi, praktisi, regulator, dan masyarakat umum tentang tantangan *cybercrime* dan tindakan antisipasi yang telah dilakukan selama ini berupa *cybersecurity*—khususnya pada *e-commerce*—perlu dilakukan penelitian literatur. Kajian literatur tentang *cybercrime* dan *cybersecurity* pada *e-commerce* diharapkan dapat memberikan gambaran tentang dinamika perkembangan domain ini. Studi

JURSIMA
Jurnal Sistem Informasi & Manajemen
ISSN : 2338-1523, E-ISSN: 2541- 576X

sebelumnya tentang *e-commerce* (Kehista *et al.*, 2023) dan masalah umum yang dihadapi oleh *e-commerce* (Rohmah, 2022) mendorong penelitian ini.

Penelitian ini dilakukan dengan mengumpulkan, memilih, ekstraksi, dan menganalisis artikel yang sesuai dengan pertanyaan penelitian. Hasilnya mencakup artikel-artikel tersebut secara keseluruhan. Hasil penelitian ini memberikan gambaran tentang *cybercrime* dan *cybersecurity* pada *e-commerce*. Hasil-hasil ini dapat digunakan sebagai acuan teori, kerangka, dan model penelitian untuk meningkatkan wawasan dan pengetahuan tentang tantangan dan antisipasi *cybercrime* dan *cybersecurity* pada *e-commerce*. Selain itu, hasil-hasil ini juga memberikan peluang untuk penelitian di masa depan.

METODE PENELITIAN

Penelitian ini dilakukan dengan menggunakan metode tinjauan pustaka matematis atau *systematic literature review* (SLR). Tahap pertama yang dilakukan pada penelitian yang menggunakan metode SLR adalah menentukan tujuan dan hasil yang diinginkan dari penelitian yang akan dilakukan. Penelitian ini dilakukan dengan tujuan untuk mengetahui bentuk tindakan *cybercrime* yang mengancam *e-commerce* dan upaya yang perlu dilakukan dalam rangka mengantisipasi ancaman tindakan tersebut. Untuk mencapai tujuan tersebut, maka dapat dirumuskan pertanyaan penelitian antara lain: (1) Bagaimana bentuk tindakan *cybercrime* yang mengancam *e-commerce*?; dan (2) Bagaimana *cybersecurity* pada *e-commerce* dalam mengantisipasi ancaman tindakan *cybercrime*?. Tahap kedua, melakukan pencarian artikel yang sehubungan dengan topik penelitian. Proses pencarian artikel dilakukan melalui Google Scholar dengan menggunakan kata kunci "*cybercrime cybersecurity e-commerce*". Tahap ketiga, peneliti melakukan pemilihan artikel yang telah diperoleh sebelumnya dari proses pencarian. Pemilihan artikel ini dilakukan dengan menggunakan bantuan aplikasi *Publish or Perish* berdasarkan kriteria-kriteria berikut: (1) Artikel yang diterbitkan dalam kurun waktu 7 tahun, yaitu dari tahun 2016 hingga tahun 2022; (2) Artikel yang mampu menjawab pertanyaan penelitian yang telah dirumuskan sebelumnya; dan (3) Artikel yang didapatkan dari sumber jurnal atau prosiding yang terindeks Sinta dan Scopus. Setelah dilakukan proses pemilihan artikel, untuk mengorganisir artikel yang telah dipilih tersebut, maka berbagai artikel tersebut didata dan disimpan ke dalam software Mendeley. Tahap terakhir, peneliti melakukan analisis terhadap isi artikel yang telah dipilih berdasarkan pertanyaan penelitian sehingga diperoleh gambaran yang menyeluruh dari bentuk tindakan *cybercrime* yang mengancam *e-commerce* dan antisipasi *cybersecurity* untuk menanggulangi ancaman tindakan tersebut.

HASIL DAN PEMBAHASAN

Hasil proses pencarian artikel dengan menggunakan kata kunci "*cybercrime cyber security e-commerce*" pada google scholar diperoleh hasil sebanyak 15.300 artikel, kemudian dari hasil tersebut dilakukan proses pemilihan artikel yang akan digunakan pada penelitian ini. Berikut rincian proses pemilihan artikel tersebut:

1. Artikel yang diterbitkan dalam kurun waktu 7 tahun, yaitu dari tahun 2016 hingga 2022. Jumlah artikel yang diperoleh sebanyak 10.500 artikel.
2. Artikel yang mampu menjawab pertanyaan penelitian yang telah dirumuskan sebelumnya. Pemilihan artikel yang mampu

JURSIMA
Jurnal Sistem Informasi & Manajemen
ISSN : 2338-1523, E-ISSN: 2541- 576X

menjawab pertanyaan penelitian ini dilakukan dengan menggunakan bantuan aplikasi *Publish or Perish* agar dapat memperoleh 10 artikel dengan kualitas terbaik untuk masing-masing pertanyaan penelitian, di mana kata kunci yang dimasukkan beserta jumlah artikelnya adalah sebagai berikut:

a. Ancaman *cybercrime* dalam *e-commerce* (*cybercrime threat in e-commerce*) sebanyak 20 artikel.
b. Peran *cybersecurity* dalam *e-commerce* (*the role of cybersecurity in e-commerce*) sebanyak 20 artikel.

3. Artikel yang bersumber dari jurnal atau prosiding yang terindeks Sinta dan Scopus. Jumlah artikel yang diperoleh sebanyak 18 artikel

Berdasarkan rincian proses pemilihan artikel di atas, terlihat bahwa jumlah artikel yang memenuhi kriteria-kriteria yang telah ditentukan adalah sebanyak 18 artikel. Namun, terdapat beberapa artikel yang tidak dapat diakses peneliti sehingga jumlah artikel yang dapat digunakan pada penelitian ini adalah sebanyak 17 artikel. Selanjutnya, artikel-artikel ini diklasifikasikan berdasarkan tahun terbit, metode penelitian yang digunakan, dan topik yang dibahas.

Pengklasifikasian artikel yang digunakan pada penelitian ini berdasarkan tahun terbit memperoleh hasil bahwa jumlah publikasi artikel yang paling banyak adalah pada tahun 2021 dan 2022 dengan 4 artikel. Sementara itu, jumlah publikasi artikel yang paling sedikit adalah pada tahun 2016 dan 2018 dengan 1 artikel. Publikasi artikel tentang *cybercrime* dan *cybersecurity* pada *e-commerce* sejak tahun 2016 hingga 2022 sangat fluktuatif dan cenderung meningkat. Hasil klasifikasi artikel berdasarkan tahun terbit ditunjukkan pada tabel 1 berikut ini:

Tabel 1. Klasifikasi Artikel Berdasarkan Tahun Terbit

Tahun	Jumlah Artikel
2016	1
2017	2
2018	1
2019	3
2020	2
2021	4
2022	4
Jumlah	17

Pengklasifikasian artikel yang digunakan pada penelitian ini berdasarkan metode penelitiannya memperoleh hasil bahwa metode yang paling banyak digunakan adalah metode survei dengan 7 artikel. Metode penelitian survei menggunakan data yang dikumpulkan melalui kuesioner, wawancara, dokumentasi, dan observasi. Hasil klasifikasi artikel berdasarkan metode penelitian ditunjukkan pada tabel 2 berikut ini:

Tabel 2. Klasifikasi Artikel Berdasarkan Metode Penelitian

Metode Penelitian	Jumlah Artikel
Literature Review	4
Systematic Literature Review	2
Metode Campuran	2
Survei	7
Desk Study	1
Pengabdian Masyarakat	1
Jumlah	17

JURSIMA
Jurnal Sistem Informasi & Manajemen
ISSN : 2338-1523, E-ISSN: 2541- 576X

Pengklasifikasian artikel yang digunakan pada penelitian ini berdasarkan topik yang dibahas memperoleh hasil bahwa secara umum topik yang dibahas pada artikel-artikel tersebut adalah mengenai tindakan cybercrime pada *e-commerce* dan antisipasi dari *cybersecurity* terhadap tindakan tersebut. Hasil klasifikasi artikel berdasarkan topik pembahasan ditunjukkan pada tabel 3 berikut ini:

Tabel 3. Klasifikasi Artikel Berdasarkan Topik Pembahasan

Topik	Jumlah Artikel	Penulis
Manajemen risiko pada *e-commerce*	1	(Toleuuly *et al.*, 2020)
Perkembangan *e-commerce*	3	(Hendarsyah, 2019; Lukito, 2017; Srisadono, 2018)
Cybercrime dan *cybersecurity* pada *fintech*	1	(Anggono *et al.*, 2021)
Pengaruh *cybercrime* terhadap pengguna *e-commerce*	4	(Apau *et al.*, 2019; Saleh *et al.*, 2017; Rahayu *et al.*, 2021; Apau dan Koranteng, 2019)
Ancaman *cybercrime* dalam *e-commerce*	3	(Munjal dan A, 2016; Isnaini dan Widodo, 2022; Ramadhan *et al.*, 2020)
Kebijakan perusahaan *cybersecurity*	1	(Mishra *et al.*, 2022)
Kesadaran konsumen mengenai *cybersecurity* dalam *e-commerce*	2	(D'adamo *et al.*, 2021a; Rohmah, 2022)
Peran *cybersecurity* bagi perkembangan ekonomi	1	(D'adamo *et al.*, 2021b)
Tantangan *cybersecurity* dalam *e-commerce*	1	(Liu *et al.*, 2022)

Masalah terbesar yang dihadapi oleh *e-commerce* adalah berbagai bentuk tindakan *cybercrime* yang dapat menghambat perkembangan bisnisnya, sehingga diperlukan adanya perjuangan ekstra dalam mengimplementasikan *cybersecurity* untuk meminimalkan peluang terjadinya tindakan *cybercrime* tersebut.

1. Tindakan *Cybercrime* pada *E-Commerce*

Di era industri 4.0 saat ini, hampir semua kegiatan masyarakat serba digital dan data menjadi sumber daya yang sangat penting dan berharga dalam melaksanakan kegiatan tersebut, termasuk kegiatan *e-commerce*. Apabila perusahaan gagal mengatasi perlindungan data yang lemah, maka hal itu dapat menjadi suatu ancaman yang serius bagi siklus bisnis perusahaan. Celah dalam sistem perlindungan data dapat menyebabkan munculnya berbagai ancaman keamanan data bagi perusahaan. Selain kerugian operasional, ancaman keamanan data ini juga berdampak negatif pada citra perusahaan secara keseluruhan, terutama jika terkait dengan data pengguna. Ancaman keamanan data semakin menjadi perhatian akhir-akhir ini, meningkatnya penggunaan internet dan perlindungan data yang lemah adalah

JURSIMA
Jurnal Sistem Informasi & Manajemen
ISSN : 2338-1523, E-ISSN: 2541- 576X

alasan mengapa ancaman keamanan data terus meningkat. Tidak ada yang bisa menjamin keamanan dari suatu sistem. Oleh karena itu, semua pihak yang terlibat dalam kegiatan berbasis data ini harus siap mengantisipasi dan merespon ancaman keamanan data.

Ancaman keamanan data umumnya disebabkan oleh adanya *cybercrime*. *Cybercrime* merupakan tindakan kriminal atau tidak bertanggung jawab yang dilakukan oleh pengguna komputer yang ingin mengambil keuntungan atas meluasnya penggunaan jaringan komputer. Hal ini tentunya dapat menimbulkan ancaman serius terhadap integritas, keamanan, dan kualitas sebagian besar sistem informasi bisnis, dan dengan demikian menjadikan pengembangan metode keamanan yang efektif sebagai prioritas utama (LEENA, 2011).

Perkembangan teknologi secara tidak langsung berdampak pada kemudahan dalam penyebaran data dan informasi. Hal ini meningkatkan risiko terjadinya *cybercrime* dalam bentuk serangan untuk mengambil data rahasia dan juga menurunkan kepercayaan antara pelanggan dengan perusahaan (Hussien *et al.*, 2022). *Cybercrime* ini tentunya akan menimbulkan ketakutan di benak banyak orang yang aktif melakukan kegiatan *e-commerce* (Rahayu *et al.*, 2021). Dalam *e-commerce*, pelanggan harus memberikan informasi pribadi mereka kepada perusahaan, sehingga perusahaan mampu mengetahui dan mencatat banyak informasi tentang pelanggan (Vasupula *et al.*, 2022). Misalnya, alamat rumah, nomor telepon, nomor rekening, tanggal lahir, dan lain sebagainya. Perusahaan juga dapat mencatat riwayat pembelian yang dilakukan oleh pelanggan dan membandingkannya dengan detail persediaan barang yang tersisa di perusahaan tersebut. Beberapa bentuk tindakan *cybercrime* yang umumnya dapat terjadi dalam *e-commerce* adalah akses tidak sah ke sistem dan layanan komputer, perubahan atau pencurian data, *distributed denial of service attacks*, penipuan kartu kredit secara online, *phishing*, *vishing*, dan *smishing* (Liu *et al.*, 2022; Khan, 2019; Saleh *et al.*, 2017; Saputra, 2016; Munjal dan A, 2016).

Transaksi yang dilakukan dalam kegiatan *e-commerce* harus aman bagi penjual dan pembeli. Saat menggunakan internet untuk bertransaksi, kepercayaan dianggap sebagai indikator yang penting dan signifikan. Keterbukaan internet yang memberikan akses kepada semua orang dapat menjadikan internet sebagai media yang terbuka untuk melakukan tindakan *cybercrime*. Selain itu, anonimitas internet dapat menyembunyikan niat dari para pelaku *cybercrime* sehingga menjadi sulit untuk mengatasi terjadinya tindakan *cybercrime* (Apau *et al.*, 2019).

Tindakan *cybercrime* telah menjadi perhatian utama di seluruh dunia. Banyak perusahaan yang kehilangan miliaran rupiah setiap tahun karena bisnis yang hilang, aset yang dicuri, dan reputasi yang rusak karena tindakan *cybercrime*. Dampak buruk dari tindakan *cybercrime* ini tidak hanya menyebabkan perusahaan mengalami kehilangan banyak uang, tetapi juga kehilangan pelanggan mereka. Tindakan *cybercrime* ini dapat merusak kepercayaan pedagang dan pelanggan dalam berbelanja online, yang dianggap sebagai kerugian yang tidak berwujud (Saleh *et al.*, 2017). Penelitian lain menyatakan bahwa perkembangan *e-commerce* menjadi terhambat karena kurangnya regulasi dan lemahnya perlindungan pelanggan terhadap tindakan *cybercrime* (Pratamasari, 2020). Oleh karena itu, baik regulator maupun pelaku bisnis menyadari bahwa perlu dilakukan suatu tindakan pencegahan kritis dan penegakan hukum yang terus mengikuti

JURSIMA
Jurnal Sistem Informasi & Manajemen
ISSN : 2338-1523, E-ISSN: 2541- 576X

bagaimana perkembangan tindakan *cybercrime* (Fahlevi *et al.*, 2019).

2. Peran *Cybersecurity* pada *E-Commerce*

Teori Keamanan Informasi atau *Information Security Theory* (IST) menyatakan bahwa "Keamanan informasi adalah proses sadar atau bawah sadar di mana orang dan organisasi berusaha untuk menciptakan sumber daya yang berkelanjutan, dari informasi" (Horne *et al.*, 2016). Sesuai dengan tujuan informasi, individu dan organisasi melindungi informasi dari risiko dan ancaman dengan menerapkan tindakan pengendalian yang sesuai. Menjaga informasi terlindungi sesuai dengan kebutuhan organisasi dan individu membuat sumber daya informasi berkelanjutan. Untuk lebih spesifik, Keamanan informasi berfokus pada perlindungan informasi, sesuai dengan jenis dan sensitivitas informasi serta penggunaan strategisnya untuk organisasi (Horne *et al.*, 2016).

Salah satu tantangan paling signifikan yang dihadapi *e-commerce* sejak awal adalah ancaman keamanan siber (Kianpour *et al.*, 2021). Keamanan siber melindungi sistem komputer dari pengungkapan informasi, penyesatan, kerusakan, atau pencurian data elektronik, perangkat lunak, atau perangkat keras (Schatz *et al.*, 2017). Dalam *e-commerce*, ini semua tentang keamanan elektronik yang terkait dengan aktivitas *e-commerce*. Perusahaan bisnis terus berinvestasi dalam teknologi untuk mencegah ancaman dunia maya, tetapi pelaku dunia maya memperoleh akses ke sistem dan data bisnis. Lanskap masalah keamanan dunia maya berkembang saat pelaku dunia maya mencari kerentanan baru melalui berbagai cara. Di satu sisi, aktor jahat meningkatkan keterampilan mereka dan di sisi lain, mereka mengadopsi teknologi dan teknik canggih untuk menargetkan berbagai organisasi (Wirth, 2017). Hampir semua organisasi yang menggunakan konektivitas internet atau komputer, termasuk layanan kesehatan, perusahaan keuangan, transportasi, pemerintah, dan industri manufaktur, menjadi sasaran terus-menerus.

Dalam beberapa tahun terakhir, Perhimpunan Bangsa Bangsa Asia Tenggara (ASEAN) telah melihat pertumbuhan yang signifikan dalam e-commerce global. Meskipun ASEAN juga diperkirakan akan menghasilkan sebagian besar pertumbuhan industri di masa depan, transaksi elektronik (transaksi elektronik) kurang berkembang di Asia Tenggara dan kesiapan infrastruktur keseluruhan untuk *e-commerce* masih dalam tahap awal di banyak negara. Singapura, Thailand, dan Malaysia berada di posisi tiga teratas dalam semua indikator yang tercantum di atas, dan di antara negara-negara CLMV, Vietnam telah membuat kemajuan signifikan dalam memfasilitasi *e-commerce* (Heejin Kim., 2019).

Di tahun 2025, perkembangan ekonomi digital ASEAN diperkirakan akan mencapai 102 miliar dolar AS. Ini karena pangsa pasar ekonomi digital menghasilkan keuntungan hingga $20 miliar pada tahun 2018 saja, menurut para ekonom. Paling tidak, serangan siber terhadap sistem informasi di Asia Tenggara dapat mengganggu dan mengacaukan ekonomi digital kawasan. Meski Singapura merupakan pusat IT Asia Tenggara, namun sebenarnya menjadi salah satu sasaran serangan siber. Berdasarkan data yang dikumpulkan oleh Tech Collective, Singapura mengalami kerugian pada tahun 2018 ketika 19.000 detail kartu kredit pelanggannya terungkap dan diperdagangkan di internet. Selain Singapura, pembobolan data juga terjadi di Vietnam saat peretas meretas data 410.000 pengguna Vietnam Airlines (Iqbal, 2019).

JURSIMA
Jurnal Sistem Informasi & Manajemen
ISSN : 2338-1523, E-ISSN: 2541- 576X

Selanjutnya, untuk artikel yang membahas mengenai *cybersecurity* terhitung sebagai:

Tabel 4. Pembahasan Artikel Mengenai *Cybersecurity*

Judul	Penulis	Resume
Analisis Keamanan Data Pribadi pada Pengguna *E-Commerce*: Ancaman, Risiko, Strategi Kemanan (*Literature Review*)	(Kehista *et al.*, 2023)	Artikel ini berfokus pada pemeriksaan bagaimana tindakan, risiko, dan strategi keamanan yang dijelaskan berdampak pada keamanan data pribadi pengguna e-niaga. Penelitian ini menggunakan metode kualitatif dan kajian pustaka (*Library Research*).
Pengenalan *Cyber Security* Sebagai Fundamental Keamanan Data Pada Era Digital	(Samudra *et al.*, 2023)	Salah satu pengenalan *Cyber Security* dan cara memasukan data pribadi pada perangkat gadget yang saat ini pelajar sudah mahir dalam menggunakan perangkat tersebut, namun masih minim pengetahuan tentang keamanan data.
The Influence of Financial Technology and E-commerce on the Success of MSMEs: Literature Review	(Lubis *et al.*, 2023)	Penelitian menggunakan sebanyak 8 artikel sebagai sumber analisis. Hasil kajian pustaka secara sistematis dari seluruh publikasi menyatakan bahwa teknologi finansial, *e-commerce*, media sosial, inovasi produk, dan literasi keuangan merupakan faktor yang mempengaruhi keberhasilan UMKM.
Pengaruh Perlindungan Data dan *Cyber Security* terhadap Tingkat Kepercayaan Menggunakan *Fintech* Masyarakat di Surabaya	(Yositya *et al.*, 2022)	Hasil dari penelitian ini disimpulkan bahwa Perlindungan data dan *cyber security* mempengaruhi tingkat kepercayaan menggunakan fintech secara signifikan.

Analisis Kesadaran *Cyber Security* Pada Kalangan Pelaku *E-Commerce* di Indonesia	(Rahmadi dan Rafie, 2020)	Hasil penelitian menunjukkan bahwa variabel pengetahuan *cyber security* terdapat hubungan yang memiliki sifat signifikan terhadap kesadaran cyber security pelaku *e-commerce*.

SIMPULAN

Penanganan kejahatan siber pada *e-commerce* harus dilakukan secara kolektif oleh pelanggan, perusahaan *e-commerce*, dan penegak hukum. Konsumen harus selalu waspada dan memastikan bahwa mereka tidak menyediakan informasi pribadi kepada orang atau organisasi yang tidak dapat dipercaya. Pada sisi perusahaan, upaya untuk meningkatkan sistem keamanan dapat dilakukan dengan mengaktifkan software pihak ketiga atau menempatkan server di *data center cloud* yang menangani segalanya di belakang layar. Perusahaan *e-commerce* juga perlu mengidentifikasi celah keamanan yang mungkin ada dalam sistem dan mengambil langkah-langkah terbaik untuk memperbaikinya secepat mungkin. Oleh karena itu, kesadaran tentang ancaman *cybercrime* pada *e-commerce* terus meningkat dan perlu dilakukan kerjasama yang erat antara pelanggan, perusahaan *e-commerce*, dan penegak hukum untuk membuat *e-commerce* lebih aman dan aman bagi semua orang. Bagi konsumen, pastikan bahwa setiap transaksi yang dilakukan melalui situs *e-commerce* dilakukan dengan hati-hati, sementara bagi perusahaan *e-commerce* pastikan pengamanan sistem yang ketat untuk benar-benar menjaga informasi pengguna tetap aman.

Cybersecurity dalam *e-commerce* mengacu pada praktik dan tindakan yang diambil untuk melindungi kerahasiaan, integritas, dan ketersediaan data dan sistem yang terlibat dalam perdagangan elektronik. Ini mencakup berbagai strategi dan teknologi yang ditujukan untuk mengamankan transaksi online, informasi pelanggan, dan keamanan platform e-commerce secara keseluruhan. Platform *e-commerce* harus memiliki situs web dan infrastruktur yang aman. Ini melibatkan penggunaan protokol enkripsi (seperti SSL/TLS) untuk melindungi data yang dikirimkan antara browser pengguna dan server. Selain itu, menerapkan *firewall*, sistem deteksi intrusi, dan pembaruan keamanan rutin dapat membantu bertahan dari ancaman dunia maya.

UCAPAN TERIMA KASIH

Puji syukur peneliti panjatkan kepada Allah SWT yang berkat rahmat dan hidayah-Nya, peneliti dapat melaksanakan dan menyelesaikan penelitian ini dengan tepat waktu. Selain itu, peneliti mengucapkan terima kasih kepada Ibu Dr. Rita Rahayu, SE, M.Si, Ak selaku dosen pengampu mata kuliah sistem informasi akuntansi dan manajemen yang telah memberikan arahan dan saran yang baik dalam penelitian ini.

DAFTAR PUSTAKA

Anggono, A., Tarjo, & Riskiyadi, M. (2021). Cybercrime dan Cybersecurity pada Fintech: Sebuah Tinjauan Pustaka Sistematis. *Jurnal Manajemen Dan Organisasi (JMO)*, *12*(3), 239–251.

Apau, R., & Koranteng, F. N. (2019). Impact of cybercrime and trust on the use of e-commerce technologies: An application of the theory of planned

behavior. *International Journal of Cyber Criminology*, *13*(2), 228–254. https://doi.org/10.5281/zenodo.3697886

Apau, R., Koranteng, F. N., & Gyamfi, S. A. (2019). Cyber-Crime and its Effects on E-Commerce Technologies. *Journal of Information*, *5*(1), 39–59. https://doi.org/10.18488/journal.104.2019.51.39.59

D'adamo, I., González-Sánchez, R., Medina-Salgado, M. S., & Settembre-Blundo, D. (2021a). E-commerce calls for cyber-security and sustainability: How european citizens look for a trusted online environment. *Sustainability (Switzerland)*, *13*(12), 1–17. https://doi.org/10.3390/su13126752

D'adamo, I., González-Sánchez, R., Medina-Salgado, M. S., & Settembre-Blundo, D. (2021b). Methodological perspective for assessing european consumers' awareness of cybersecurity and sustainability in e-commerce. *Sustainability (Switzerland)*, *13*(20), 1–10. https://doi.org/10.3390/su132011343

Fahlevi, M., Saparudin, M., Maemunah, S., Irma, D., & Ekhsan, M. (2019). Cybercrime Business Digital in Indonesia. *E3S Web of Conferences*, *125*(November). https://doi.org/10.1051/e3sconf/201912521001

Firmansyah Putri, D. D., & Fahrozi, M. H. (2021). Upaya Pencegahan Kebocoran Data Konsumen melalui Pengesahan RUU Perlindungan Data Pribadi (Studi Kasus E-Commerce Bhinneka.Com). *Borneo Law Review*, *5*(1), 46–68. https://doi.org/10.35334/bolrev.v5i1.2014

Hendarsyah, D. (2019). E-Commerce Di Era Industri 4.0 Dan Society 5.0. *IQTISHADUNA: Jurnal Ilmiah Ekonomi Kita*, *8*(2), 171–184. https://doi.org/10.46367/iqtishaduna.v8i2.170

Horne, C. A., Ahmad, A., & Maynard, S. B. (2016). A Theory on Information Security. *Australasian Conference on Information Systems*, *July 2017*, 1–12.

Hussien, F. T. A., Rahma, A. M. S., & Wahab, H. B. A. (2022). Design and implement a new secure prototype structure of e-commerce system. *International Journal of Electrical and Computer Engineering*, *12*(1), 560–571. https://doi.org/10.11591/ijece.v12i1.pp560-571

Isnaini, K., & Widodo, W. (2022). Literasi Digital Bagi Komunitas Digital Marketer Purwokerto Dalam Upaya Mencegah Ancaman Keamanan Data Di Dunia Siber. *SELAPARANG: Jurnal Pengabdian Masyarakat Berkemajuan*, *6*(4), 1795. https://doi.org/10.31764/jpmb.v6i4.10764

Kehista, A. P., Fauzi, A., Tamara, A., Putri, I., & Afni, N. (2023). *Analisis Keamanan Data Pribadi pada Pengguna E-Commerce : Ancaman , Risiko , Strategi Kemanan (Literature Review)*. *4*(5), 625–632.

Khan, S. W. (2019). Cyber Security Issues and Challenges in E-Commerce. *SSRN Electronic Journal*, 1197–1204. https://doi.org/10.2139/ssrn.3323741

Kianpour, M., Kowalski, S. J., & Øverby, H. (2021). Systematically understanding cybersecurity economics: A survey. *Sustainability (Switzerland)*, *13*(24). https://doi.org/10.3390/su132413677

LEENA, N. (2011). Cyber Crime Effecting E-commerce Technology. *Oriental Journal of Computer Science and Technology*, *4*(1), 209–212.

http://www.computerscijournal.org/dnload/N. Leena/OJCSV04I01P209-212.pdf

Liu, X., Ahmad, S. F., Anser, M. K., Ke, J., Irshad, M., Ul-Haq, J., & Abbas, S. (2022). Cyber security threats: A never-ending challenge for e-commerce. *Frontiers in Psychology*, *13*(October), 1–15. https://doi.org/10.3389/fpsyg.2022.927398

Lubis, R., Canggih, R. R., Permesti, M., Leonardo, E., & Nurmala, E. (2023). *The Influence of Financial Technology and E-commerce on the Success of MSMEs : Literature Review*. *1*(January), 1058–1079.

Lukito, I. (2017). Tantangan Hukum dan Peran Pemerintah dalam Pembangunan E-Commerce (Legal Challenges and Government`S Role in E-Commerce Development). *Pusat Pengkajian Dan Pengembangan Kebijakan Badan Penelitian Dan Pengembangan Hukum Dan HAM Kementerian Hukum Dan HAM R.I.*, *11*(3), 349–367.

Mishra, A., Alzoubi, Y. I., Gill, A. Q., & Anwar, M. J. (2022). Cybersecurity Enterprises Policies: A Comparative Study. *Sensors*, *22*(2), 1–35. https://doi.org/10.3390/s22020538

Munjal, S., & A, A. (2016). Cyber Crimes Threat for the E-Commerce. *SSRN Electronic Journal*, *3*(1). https://doi.org/10.2139/ssrn.2767443

Nafi'ah, R. (2020). Pelanggaran Data Dan Pencurian Identitas Pada E-Commerce. *CyberSecurity Dan Forensik Digital*, *3*(1), 7–13.

Pratamasari, A. (2020). Cybersecurity and Custom Regulations as Trade Barriers in ASEAN e-Commerce: Case of Indonesian e-Commerce. *Jurnal Global & Strategis*, *14*(1), 1. https://doi.org/10.20473/jgs.14.1.2020.1-16

Putri, N. I., Komalasari, R., & Munawar, Z. (2020). PENTINGNYA KEAMANAN DATA DALAM INTELIJEN BISNIS. *Jurnal Sistem Informasi*, *01*(02).

Rabiah, A. S., Fahlevi, M., Juhandi, N., & Winarto, P. (2020). Haruskah E-Payment Trust Diterapkan E-Commerce Sebagai Faktor Kepuasan Konsumen? *E-Jurnal Manajemen Universitas Udayana*, *9*(7), 2724–2743. https://doi.org/10.24843/ejmunud.2020.v09.i07.p13

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), 632–637. https://doi.org/10.52362/jisamar.v5i3.478

Rahmadi, G., & Rafie, A. (2020). *Analisis Kesadaran Cyber Security pada Kalangan Pelaku e-Commerce di Indonesia*.

Ramadhan, M., Ariyanti, D. O., & Ariyani, N. (2020). Pencurian e-money pada e-commerce dalam Tindak Pidana Cybercrime sebagai Tindak Pidana Ekonomi. *Reformasi Hukum*, *24*(2), 169–188. https://doi.org/10.46257/jrh.v24i2.179

Rohmah, R. N. (2022). Upaya Membangun Kesadaran Keamanan Siber pada Konsumen E-commerce di Indonesia. *Cendekia Niaga: Journal of Trade Development and Studies*, *6*(1), 1–11.

Saleh, H., Rezk, A., & Barakat, S. (2017). The Impact of Cyber Crime on E-Commerce. *International Journal of Intelligent Computing and Information Sciences*, *17*(3), 85–96. https://doi.org/10.21608/ijicis.2017.30055

Samudra, Y., Hidayat, A., & Wahyu, M. F.

(2023). Pengenalan Cyber Security Sebagai Fundamental Keamanan Data Pada Era Digital. *AMMA : Jurnal Pengabdian Masyarakat*, *1*(12), 1594–1601. https://journal.mediapublikasi.id/index.php/amma

Saputra, R. W. (2016). A survey of cyber crime in Indonesia. *2016 International Conference on ICT for Smart Society, ICISS 2016, July 2016*, 1–5. https://doi.org/10.1109/ICTSS.2016.7792846

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a More Representative Definition of Cyber Security. *The Journal of Digital Forensics, Security and Law*, *12*(2). https://doi.org/10.15394/jdfsl.2017.1476

Srisadono, W. (2018). Strategi Perusahaan E-Commerce Membangun Brand Community Di Media Sosial Dalam Meningkatkan Omset Penjualan. *Jurnal Pustaka Komunikasi, 1*(1), 167–179. https://journal.moestopo.ac.id/index.php/pustakom/article/viewFile/552/279

Toleuuly, A., Yessengeldin, B., Khussainova, Z., Yessengeldina, A., Zhanseitov, A., & Jumabaeva, S. (2020). Features of E-Commerce Risk Management. *Academy of Strategic Management Journal*, *19*(1), 6104.

Vasupula, N., Munnangi, V., & Daggubati, S. (2022). *Modern Privacy Risks and Protection Strategies in Data Analytics BT - Soft Computing and Signal Processing* (V. S. Reddy, V. K. Prasad, J. Wang, & K. T. V Reddy (eds.); pp. 81–89). Springer Singapore.

Wajong, A. M. R., & Putri, C. R. (2010). KEAMANAN DALAM ELECTRONIC COMMERCE PENDAHULUAN. *ComTech*, *1*(2), 867–874.

Wirth, A. (2017). The economics of cybersecurity. *Biomedical Instrumentation & Technology*, 52–59.

Yositya, A., Mauliza, I., Dwi, R., Machmudi, S., & Indrarini, R. (2022). Pengaruh Perlindungan Data Dan Cyber Security Terhadap Tingkat Kepercayaan Menggunakan Fintech Masyarakat Di Surabaya. *Sibatik Journal | Volume*, *1*(11), 2497–2516. https://publish.ojs-indonesia.com/index.php/SIBATIK