STRATEGI MANAJEMEN RISIKO SIBER DALAM PERUSAHAAN E- COMMERCE DI INDONESIA: TINJAUAN SISTEMATIS DAN PERBANDINGAN DENGAN PRAKTIK GLOBAL

Farisah Keke Nola Padang[1], Aryadino Anggara[2] , Nur Abdullah Gimnastiar[3] , nicholas faisal simanjuntak[4] , Ahmed Charesyah Lbs[5] Arsyadona[6]
farisahkekepadang21@gmail.com [1] , ariadino14@gmail.com [2] , abdullahgimnastiar1717@gmail.com [3] , nicholasfaisal28@gmail.com [4] , lubisarel@gmail.com [5] , arsyadona1100000174@uinsu.ac.id [6]
123456Fakultas Ekonomi dan Bisnis Islam, Universitas Islam Negeri Sumatera Utara, Indonesia

Abstrak
Abstrak: Manajemen risiko siber menjadi penting bagi perusahaan e-commerce untuk melindungi data dan kepercayaan konsumen. Penelitian ini menganalisis strategi manajemen risiko siber di perusahaan e-commerce Indonesia dan membandingkannya dengan praktik global melalui tinjauan sistematis literatur dari tahun 2014 hingga 2024. Temuan menunjukkan bahwa perusahaan global cenderung menggunakan pendekatan proaktif dengan teknologi mutakhir, sedangkan perusahaan Indonesia, terutama UMKM, masih mengandalkan metode tradisional yang kurang efektif. Meskipun ada regulasi pemerintah seperti Peraturan Pemerintah No. 71 Tahun 2019, implementasinya masih kurang optimal. Penelitian ini merekomendasikan adopsi teknologi dan penerapan standar keamanan yang lebih ketat untuk meningkatkan ketahanan perusahaan e-commerce Indonesia terhadap ancaman siber.
Kata Kunci: Manajemen Risiko Siber, E-commerce, Indonesia, Teknologi, Kebijakan Pemerintah.
Abstract: Cyber risk management is important for e-commerce companies to protect data and consumer trust. This study analyzes cyber risk management strategies in Indonesian e- commerce companies and compares them with global practices through a systematic review of literature from 2014 to 2024. The findings show that global companies tend to use a proactive approach with cutting-edge technology, while Indonesian companies, especially MSMEs, still rely on traditional methods that are less effective. Despite government regulations such as Government Regulation No. 71/2019, implementation is still suboptimal. This research recommends technology adoption and stricter implementation of security standards to improve the resilience of Indonesian e-commerce companies to cyber threats.
Keywords: Cyber Risk Management, E-commerce, Indonesia, Technology, Government Policy.

Article History
Received: Januari 2025
Reviewed: Januari 2025
Published: Januari 2025

Plagirism Checker No 234
Prefix DOI : Prefix DOI : 10.8734/Kohesi.v1i2.365
Copyright : Author
Publish by : Kohesi

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License

PENDAHULUAN

Di tengah perkembangan pesat teknologi dan digitalisasi, ancaman siber telah menjadi perhatian utama perusahaan di seluruh dunia. Perusahaan e- commerce menghadapi risiko tinggi terhadap serangan siber, termasuk pencurian data, penyalah gunaan informasi

pelanggan, dan penipuan identitas yang dapat merugikan finansial serta mengurangi kepercayaan konsumen (Johnson et al., 2019). Mengingat banyaknya data sensitif yang diproses dan disimpan, sektor e-commerce menjadi target empuk bagi aktor-aktor kejahatan siber. Selain itu, kompleksitas lingkungan siber global memperburuk situasi ini, dengan ancaman yang semakin berkembang secara cepat dan sulit untuk dikelola hanya dengan pendekatan konvensional (Varma & Marwah, 2020). Oleh karena itu, perusahaan perlu mengimplementasikan strategi manajemen risiko siber yang proaktif untuk melindungi infrastruktur digital mereka dari serangan yang merugikan.

Di Indonesia, perusahaan e-commerce menghadapi sejumlah tantangan unik terkait manajemen risiko siber. Beberapa masalah utama yang perlu diperhatikan antara lain: (1) minimnya standar keamanan yang seragam, (2) kurangnya kesadaran dan pemahaman karyawan tentang pentingnya keamanan siber, (3) keterbatasan anggaran dan sumber daya untuk investasi keamanan yang memadai, dan (4) kerentanan infrastruktur teknologi yang sering tidak mengikuti perkembangan ancaman terbaru (Setyawan, 2022). Selain itu, banyak perusahaan masih belum memiliki kebijakan manajemen risiko siber yang jelas atau mengintegrasikan praktik global terbaik dalam prosedur keamanan mereka (Nugroho et al., 2023). Penelitian ini perlu dilakukan untuk mengeksplorasi praktik terbaik dari skala global yang dapat diterapkan dalam konteks Indonesia, dengan tujuan untuk memperkuat upaya perlindungan terhadap risiko yang terus meningkat di sektor ini.

Penelitian sebelumnya menunjukkan bahwa strategi manajemen risiko siber yang efektif dapat secara signifikan mengurangi dampak negatif serangan siber terhadap perusahaan e-commerce. Misalnya, studi dari Lee dan Choi (2018) mengindikasikan bahwa adopsi pendekatan manajemen risiko yang proaktif membantu meningkatkan ketahanan perusahaan dalam menghadapi serangan siber. Selain itu, hasil penelitian dari Kumar & Srivastava (2020) mendukung pentingnya penerapan strategi keamanan yang terstruktur dalam lingkungan bisnis yang memiliki risiko tinggi seperti e-commerce. Di Indonesia, dasar kuat untuk penelitian ini juga datang dari kebijakan pemerintah yang semakin berfokus pada peningkatan keamanan siber, seperti yang tertuang dalam Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Kementerian Komunikasi dan Informatika, 2019). Kebijakan ini mendorong perusahaan untuk memperkuat sistem keamanan mereka demi melindungi data pelanggan dan menjamin keberlangsungan transaksi elektronik.

Dalam konteks Indonesia, banyak perusahaan e-commerce belum memiliki strategi yang komprehensif untuk menghadapi ancaman siber. Menurut studi oleh Suwandi (2021), sebagian besar pelaku bisnis e-commerce masih dalam tahap awal pengembangan program manajemen risiko siber, dan upaya mereka sering kali bersifat reaktif, yaitu hanya bertindak ketika terjadi insiden. Penelitian ini penting dilakukan agar dapat mengidentifikasi praktik global terbaik yang sesuai dengan kondisi perusahaan di Indonesia. Selain itu, penguatan strategi manajemen risiko siber akan membantu perusahaan dalam memitigasi ancaman sekaligus menjaga kepercayaan pelanggan.

Secara global, perusahaan e-commerce telah mulai menerapkan berbagai pendekatan untuk menghadapi ancaman siber. Tren terbaru menunjukkan peningkatan penggunaan teknologi seperti kecerdasan buatan dan pembelajaran mesin dalam mendeteksi serta merespons ancaman secara lebih efektif (Wang & Li, 2022). Strategi ini memungkinkan deteksi dini terhadap potensi ancaman dan mengurangi kemungkinan serangan berdampak besar pada sistem. Namun, implementasi teknologi ini membutuhkan investasi besar dan kapasitas sumber daya manusia yang memadai. Oleh karena itu, studi komparatif terhadap praktik global yang relevan diharapkan mampu memberikan wawasan baru bagi perusahaan e-commerce di Indonesia.

Sejumlah penelitian menunjukkan bahwa integrasi praktik global dalam manajemen risiko siber dapat memberikan keuntungan signifikan bagi perusahaan e-commerce di negara

berkembang, termasuk Indonesia. Misalnya, Setyawan dan Pratama (2023) menemukan bahwa penerapan standar keamanan siber internasional mampu meningkatkan keandalan sistem dan kepercayaan konsumen. Selain itu, pemerintah Indonesia melalui berbagai kebijakan juga mendorong adopsi standar keamanan yang lebih baik untuk melindungi sektor-sektor penting dalam perekonomian digital.

Tujuan dari penelitian ini adalah untuk melakukan tinjauan sistematis terhadap strategi manajemen risiko siber yang diterapkan oleh perusahaan e commerce di Indonesia dan membandingkannya dengan praktik global yang ada. Hasil penelitian ini diharapkan dapat memberikan rekomendasi yang dapat meningkatkan ketahanan siber perusahaan e-commerce Indonesia. Dengan demikian, penelitian ini tidak hanya bertujuan untuk mendukung upaya perlindungan data pelanggan dan keamanan sistem, tetapi juga untuk mendorong perusahaan e-commerce di Indonesia dalam mengadopsi praktik keamanan yang lebih efektif dan berkelanjutan.

KAJIAN TEORI

1. Manajemen Risiko Siber

Manajemen risiko siber adalah proses identifikasi, penilaian, dan mitigasi risiko-risiko yang terkait dengan keamanan informasi dan sistem teknologi (Whitman & Mattord, 2017). Dalam konteks perusahaan e-commerce, manajemen risiko siber sangat penting karena banyak data sensitif pelanggan yang disimpan dalam sistem online, termasuk informasi pribadi dan finansial. Peningkatan ancaman siber global telah membuat manajemen risiko siber menjadi prioritas utama untuk memastikan kelangsungan bisnis dan perlindungan data pelanggan (Soomro et al., 2016). Dengan menerapkan manajemen risiko siber yang efektif, perusahaan dapat mengurangi kerugian finansial dan reputasi yang timbul dari insiden siber (Böhme & Schwartz, 2021).

2. Ancaman Siber pada E-commerce

Ancaman siber yang dihadapi perusahaan e-commerce meliputi berbagai jenis serangan, seperti serangan malware, phishing, dan ransomware. Ancaman ini memiliki dampak besar, terutama karena perusahaan e-commerce menyimpan informasi pribadi dan keuangan yang menarik bagi penjahat siber (Kumar & Srivastava, 2020). Serangan ransomware, misalnya, dapat mengunci data penting dan memeras perusahaan untuk membayar sejumlah uang sebagai tebusan. Serangan phishing, di sisi lain, berfokus pada mencuri informasi login atau detail kartu kredit pelanggan (Verizon Data Breach Investigations Report, 2023).

3. Kerentanan Infrastruktur Teknologi dalam E-commerce di Indonesia

Di Indonesia, perusahaan e-commerce sering menghadapi tantangan berupa kerentanan infrastruktur teknologi yang bisa menyebabkan kesulitan dalam mengimplementasikan sistem keamanan mutakhir. Faktor seperti minimnya standar keamanan dan keterbatasan anggaran memperparah risiko keamanan (Nugroho et al., 2023). Selain itu, banyak perusahaan e-commerce yang masih menggunakan sistem teknologi yang tidak mutakhir, yang rentan terhadap berbagai ancaman siber (Setyawan, 2022).

4. Standar Internasional dan Praktik Terbaik dalam Manajemen Risiko Siber

Standar internasional seperti ISO/IEC 27001 memberikan pedoman untuk membangun sistem manajemen keamanan informasi yang efektif. Standar ini berfokus pada perlindungan kerahasiaan, integritas, dan ketersediaan informasi, yang penting untuk melindungi aset perusahaan e-commerce (Humphreys, 2016). Dalam beberapa tahun terakhir, praktik-praktik terbaik dalam manajemen risiko siber juga mencakup adopsi teknologi baru seperti kecerdasan buatan (AI) dan pembelajaran mesin (machine learning) untuk meningkatkan ketepatan dan kecepatan deteksi ancaman (Wang & Li, 2022).

5. Kebijakan Pemerintah Indonesia dalam Keamanan Siber

Pemerintah Indonesia telah mengeluarkan beberapa kebijakan untuk meningkatkan keamanan siber, seperti Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan

Sistem dan Transaksi Elektronik. Kebijakan ini mewajibkan perusahaan untuk memastikan sistem dan transaksi elektronik mereka memenuhi standar keamanan yang ditetapkan (Kementerian Komunikasi dan Informatika, 2019). Hal ini menunjukkan komitmen pemerintah dalam melindungi data pribadi pengguna serta mendorong perusahaan untuk mengadopsi sistem keamanan yang lebih kuat (Suhendar, 2020).

6. **Perlunya Penelitian Strategi Manajemen Risiko Siber dalam Konteks Lokal**

Penelitian dalam strategi manajemen risiko siber sangat dibutuhkan di Indonesia, terutama dalam sektor e-commerce, karena karakteristik pasar yang berbeda dari negara-negara maju. Menurut penelitian Setiawan (2021), perusahaan e-commerce di Indonesia sering mengadopsi pendekatan reaktif, yaitu menanggapi ancaman setelah insiden terjadi, ketimbang pendekatan proaktif yang lebih berorientasi pada pencegahan. Oleh karena itu, studi tentang integrasi praktik global yang relevan sangat penting untuk membantu perusahaan di Indonesia meningkatkan ketahanan terhadap serangan siber (Setiawan, 2021; Suwandi, 2023).

METODE PENELITIAN

Systematic Literature Review (SLR) dipilih sebagai metode utama untuk mengidentifikasi, mengumpulkan, dan menganalisis penelitian terkait manajemen risiko siber yang telah diterapkan pada perusahaan e-commerce di Indonesia dan dunia. SLR merupakan metode yang sistematis dalam mengidentifikasi, mengevaluasi, dan menyintesis temuan dari berbagai literatur yang relevan, sehingga memungkinkan penelitian ini untuk menghasilkan pandangan yang komprehensif dan terpercaya tentang topik yang dikaji (Kitchenham & Charters, 2007).

Penelitian ini menggunakan database akademik utama, seperti IEEE Xplore, ScienceDirect, Scopus, dan Google Scholar, yang dianggap memiliki koleksi artikel terpercaya. Database ini dipilih untuk memastikan bahwa studi yang ditinjau memiliki kualitas yang tinggi dan telah melalui proses peer-review.

HASIL DAN PEMBAHASAN

Result (Temuan)

Penelitian ini menunjukkan bahwa perusahaan e-commerce global telah mengadopsi berbagai teknologi mutakhir dalam mengidentifikasi risiko siber, seperti kecerdasan buatan (AI) dan analisis big data, yang memungkinkan deteksi anomali dan aktivitas mencurigakan secara real-time (Wang & Li, 2022). Sementara itu, di Indonesia, sebagian besar perusahaan e-commerce, terutama yang berukuran kecil hingga menengah, masih mengandalkan pendekatan manual dan tradisional untuk mengidentifikasi ancaman siber. Pendekatan ini dinilai kurang efektif dan sangat rentan terhadap kesalahan manusia, yang dapat menyebabkan kerentanan terhadap serangan siber (Setyawan, 2022).

Dalam hal penilaian risiko, perusahaan e-commerce global menggunakan pendekatan berbasis risiko yang komprehensif untuk mengukur probabilitas dan dampak dari berbagai ancaman potensial (Lee & Choi, 2018). Di sisi lain, sebagian besar perusahaan e-commerce di Indonesia, khususnya Usaha Mikro, Kecil, dan Menengah (UMKM), belum menerapkan penilaian risiko secara menyeluruh. Perusahaan-perusahaan ini lebih mengandalkan strategi reaktif, yakni hanya memperbaiki sistem keamanan mereka setelah insiden terjadi, yang menunjukkan ketidaksiapan dalam menghadapi potensi ancaman (Setiawan, 2021).

Selanjutnya, dalam penerapan kontrol dan tindakan mitigasi, perusahaan e commerce global telah mengadopsi standar keamanan internasional seperti ISO/IEC 27001, yang mencakup enkripsi data, sistem deteksi intrusi, dan firewall canggih (Humphreys, 2016). Di Indonesia, banyak perusahaan masih mengandalkan kontrol dasar seperti firewall dan antivirus tanpa adanya pemantauan yang berkelanjutan, sehingga rentan terhadap ancaman siber yang tidak terdeteksi (Nugroho et al., 2023). Dalam pemantauan risiko, perusahaan global memiliki sistem pemantauan real-time yang memungkinkan deteksi dini terhadap aktivitas anomali dan memiliki tim keamanan siber yang didedikasikan untuk memantau ancaman (Varma & Marwah,

2020). Sebaliknya, di Indonesia, kebanyakan perusahaan e-commerce belum memiliki sistem pemantauan yang memadai, terutama di kalangan UMKM, yang sering kali kekurangan sumber daya dan keterampilan teknis.

Selain itu, Pemerintah Indonesia telah menerapkan Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik untuk meningkatkan standar keamanan siber di perusahaan e-commerce. Peraturan ini mendorong perusahaan untuk memenuhi standar tertentu dalam perlindungan data pelanggan, meskipun implementasinya di lapangan masih memerlukan pengawasan dan peningkatan lebih lanjut (Kementerian Komunikasi dan Informatika, 2019).

Discussion (Pembahasan)

Perbedaan yang signifikan antara praktik manajemen risiko siber di perusahaan e-commerce di Indonesia dan praktik global menunjukkan adanya kesenjangan yang perlu segera diatasi. Di tingkat global, penggunaan teknologi canggih seperti AI dan big data dalam mendeteksi risiko siber sudah menjadi standar, namun adopsi teknologi ini masih terbatas di Indonesia, khususnya di kalangan UMKM yang sering kali terkendala oleh anggaran dan keterbatasan sumber daya (Wang & Li, 2022; Setyawan, 2022). Hal ini menandakan pentingnya dukungan pemerintah dan penyediaan sumber daya teknologi yang lebih baik untuk membantu perusahaan e-commerce di Indonesia mengadopsi teknologi yang diperlukan guna meningkatkan identifikasi dan pencegahan risiko siber.

Pendekatan proaktif dalam penilaian risiko yang banyak diterapkan oleh perusahaan global juga menyoroti pentingnya kesiapan dalam mengidentifikasi potensi ancaman sebelum terjadi insiden. Di Indonesia, pendekatan yang lebih reaktif dan terbatas pada perusahaan besar menunjukkan bahwa UMKM masih belum menyadari pentingnya strategi penilaian risiko yang komprehensif. Hal ini kemungkinan besar disebabkan oleh kurangnya pengetahuan tentang manajemen risiko siber, serta anggaran dan sumber daya yang terbatas (Lee & Choi, 2018; Setiawan, 2021).

Dalam hal implementasi standar keamanan internasional, seperti ISO/IEC 27001, perusahaan e-commerce di Indonesia belum banyak yang menerapkannya. Rendahnya adopsi standar ini, khususnya di kalangan UMKM, menunjukkan bahwa kesadaran akan pentingnya keamanan siber masih perlu ditingkatkan. Perusahaan e-commerce di negara-negara maju telah berhasil menerapkan standar ini sebagai upaya untuk memperkuat keamanan data dan melindungi pelanggan, sementara di Indonesia banyak perusahaan hanya menerapkan kontrol dasar yang tidak memadai dalam menghadapi ancaman yang lebih canggih (Humphreys, 2016; Nugroho et al., 2023).

Peran kebijakan pemerintah sangat penting dalam mendorong peningkatan standar keamanan siber di sektor e-commerce. Kebijakan seperti Peraturan Pemerintah No. 71 Tahun 2019 telah memberikan landasan hukum yang kuat bagi pengembangan sistem keamanan siber, tetapi efektivitas kebijakan ini dalam praktik masih terbatas. Beberapa negara maju memiliki regulasi yang lebih ketat dan sistem penegakan hukum yang lebih efektif, yang mendorong perusahaan e-commerce untuk lebih serius dalam manajemen risiko siber mereka. Hal ini menunjukkan perlunya peningkatan penegakan hukum dan kesadaran di kalangan pelaku industri untuk memastikan kepatuhan terhadap standar keamanan (Kementerian Komunikasi dan Informatika, 2019; Whitman & Mattord, 2017).

Di tingkat global, kesiapan dalam menghadapi dan memulihkan diri dari insiden siber merupakan prioritas utama perusahaan e-commerce. Rencana respons insiden yang matang dapat membantu perusahaan mengurangi dampak dari serangan siber dan menjaga operasional bisnis tetap stabil. Di Indonesia, banyak perusahaan e-commerce masih kurang dalam hal kesiapan dan ketahanan terhadap serangan siber, terutama di kalangan UMKM. Hal ini menandakan pentingnya pelatihan dan pengembangan tim keamanan siber yang khusus untuk

memantau, merespons, dan memulihkan sistem jika terjadi serangan siber (Ahmad et al., 2022; Suhendar, 2020).

Secara keseluruhan, studi ini merekomendasikan bahwa perusahaan e commerce di Indonesia perlu meningkatkan adopsi teknologi deteksi risiko yang lebih maju, meningkatkan pelatihan karyawan terkait keamanan siber, dan mempertimbangkan untuk menerapkan standar keamanan internasional. Pemerintah dapat mendukung inisiatif ini dengan memberikan insentif dan pelatihan bagi UMKM, serta memperkuat penegakan regulasi yang telah ditetapkan untuk meningkatkan keamanan siber di sektor e-commerce Indonesia.

KESIMPULAN

Kesimpulan dari kajian ini menunjukkan bahwa terdapat perbedaan signifikan dalam strategi manajemen risiko siber antara perusahaan e-commerce di Indonesia dan praktik global. Perusahaan e-commerce internasional umumnya menerapkan pendekatan yang lebih proaktif, dengan memanfaatkan teknologi canggih seperti kecerdasan buatan dan analisis big data untuk mendeteksi dan mengelola ancaman siber secara real-time. Di sisi lain, sebagian besar perusahaan e-commerce di Indonesia, terutama UMKM, masih mengandalkan pendekatan yang lebih tradisional dan reaktif dalam menghadapi risiko siber, yang menyebabkan kerentanan terhadap serangan yang lebih kompleks.

Implementasi standar keamanan internasional seperti ISO/IEC 27001 juga masih rendah di Indonesia, sehingga banyak perusahaan hanya menggunakan kontrol dasar yang belum cukup dalam menghadapi ancaman siber modern. Hal ini memperlihatkan bahwa kesadaran dan pengetahuan tentang pentingnya keamanan siber masih perlu ditingkatkan, terutama di kalangan perusahaan kecil hingga menengah. Selain itu, meskipun pemerintah Indonesia telah menetapkan regulasi terkait keamanan siber, seperti Peraturan Pemerintah No. 71 Tahun 2019, pelaksanaannya di lapangan masih memerlukan pengawasan dan peningkatan lebih lanjut untuk mendorong kepatuhan dan penerapan standar keamanan yang lebih efektif.

Berdasarkan temuan ini, direkomendasikan agar perusahaan e-commerce di Indonesia mengadopsi teknologi deteksi dan manajemen risiko yang lebih maju serta menerapkan standar keamanan yang diakui secara internasional. Pemerintah juga berperan penting dalam memberikan dukungan, baik melalui insentif maupun pelatihan, agar UMKM dapat meningkatkan sistem keamanan sibernya. Dengan langkah-langkah tersebut, diharapkan sektor e-commerce di Indonesia dapat menjadi lebih tangguh dalam menghadapi tantangan siber yang semakin kompleks dan berkembang pesat.

DAFTAR PUSTAKA

Ahmad, A., Maynard, S. B., & Shanks, G. (2022). Incident Response Management in the Age of Cyber Warfare: Insights for E-commerce. *Journal of Information Warfare, 21(1)*, 12 25.

Alotaibi, M. (2020). Cybersecurity Risk Management Framework for E-commerce Companies: Challenges and Solutions. *International Journal of Information Security, 19(4)*, 357-367.

Böhme, R., & Schwartz, G. (2021). Cybersecurity risk management: strategic and tactical decisions. *ACM Computing Surveys, 54(3),* 1-29.

Humpreys, E. (2016). Information security management standards: Compliance, governance, and risk management. *Computers & Security, 56,* 67-77.

Ibrahim, A., & Saleh, M. (2021). Assessing the Impact of Cybersecurity Policies on E commerce Growth in Indonesia. *Journal of Cyber Policy, 6(2),* 165-182.

Johnson, R., Smith, K., & Lee, M. (2019). Cyber Risk Management in E-commerce: A Global Overview. *Journal of Cybersecurity, 5(3),* 112-129.

Kementerian Komunikasi dan Informatika. (2019). *Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik*.

Kumar, A., & Srivastava, D. (2020). Structured Cybersecurity in High-Risk Business Environments. *Journal of Business Continuity and Emergency Planning, 8(1),* 67-89.

Lee, H., & Choi, S. (2018). Proactive Risk Management in E-commerce Companies: The Importance of Strategy. *International Journal of Information Systems, 12(4),* 231-250.

NIST (2018). *Cybersecurity Framework Version 1.1.* National Institute of Standards and Technology.

Nugroho, R., Rahman, A., & Mardiana, M. (2023). Assessing Cybersecurity Measures in Indonesian E-commerce: A Case Study Approach. *International Journal of Cybersecurity and Digital Forensics, 12(1),* 44-59.

Ruan, K., Douglas, J., & Lightfoot, J. (2019). Cybersecurity Threats and Risk Assessment in the Digital Economy. *Journal of Digital Security, 12(2),* 56-74.

Setiawan, R. (2021). Challenges and Opportunities in Cybersecurity for E-commerce in Indonesia. *Journal of Southeast Asian E-commerce, 8(3),* 198-214.

Setyawan, A. (2022). Cybersecurity Challenges in Indonesian E-commerce Companies. *Indonesian Journal of Information Security, 4(1),* 23-39.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management, 36(2),* 215-225.

Stine, K., Quinn, S., & Witte, G. (2018). *Guide for Conducting Risk Assessments (NIST Special Publication 800-30 Rev. 1).* National Institute of Standards and Technology.

Suhendar, R. (2020). Implementasi Peraturan Pemerintah No. 71 Tahun 2019 dalam Keamanan Siber di Indonesia. *Jurnal Kebijakan Teknologi, 5(2),* 88-97.

Suwandi, T. (2021). Current Cybersecurity Strategies in Indonesian E-commerce Companies. *Cybersecurity Journal Indonesia, 9(2),* 94-107.

Varma, R., & Marwah, S. (2020). Cybersecurity Challenges in E-commerce: A Comparative Analysis. *Global Journal of Business Research, 14(1),* 27-38.

Wang, X., & Li, Y. (2022). AI and Machine Learning for Cybersecurity: A New Era in E commerce. *Journal of Advanced Digital Security, 14(1),* 56-78.

Whitman, M. E., & Mattord, H. J. (2017). *Principles of Information Security (6th ed.).* Cengage Learning.