AJEMB
AMERICAN JOURNAL OF ECONOMIC AND MANAGEMENT BUSINESS

American Journal of Economic and Management Business
e-ISSN: 2835-5199
Vol. 4 No. 12 December 2025

Strengthening Digital Marketing Performance of E- Commerce X in Indonesia Through Cybersecurity and Personal Data Protection

Derio Aulia Ramadhan[1*], Helni Mutiarsih Jumhur[2], Arief Arianto[3]
Universitas Telkom, Indonesia
Email: deriooaulia@gmail.com*, helnimj@telkomuniversity.ac.id

Abstract

In the digital era marked by the rapid growth of online transactions, e-commerce platforms like E-Commerce X play a central role in the modern commerce landscape. Continuous efforts to improve digital marketing performance are crucial for maintaining competitiveness and attracting consumers' attention. This research focuses on the premise that strengthening cybersecurity and compliance with the Personal Data Protection Law (PDP) is not just a compliance or technical aspect but rather a strategic pillar that significantly strengthens E-Commerce X's digital marketing. This trust is an important asset in the success of various digital marketing campaigns, from personalizing the user experience to driving transactions and loyalty. Furthermore, the study argues that compliance with the PDP Act not only mitigates legal risks but also enhances E-Commerce X's brand image as a responsible entity that respects user privacy. Thus, this research puts forward the idea that investment in robust cybersecurity and commitment to the PDP Act are integral elements in E-Commerce X's successful digital marketing strategy. This research was conducted using a descriptive qualitative method to describe in depth the relationships among website traffic volume, social media engagement, brand trust, and the implementation of cybersecurity and compliance with personal data regulations.

Keywords: digital marketing, cybersecurity, E- Commerce X , pdp law, e-commerce

INTRODUCTION

Digital transformation has fundamentally changed the global trade paradigm, with e-commerce platforms becoming the backbone of the digital economy in various countries, including Indonesia. In the Indonesian context, the growth of e-commerce has followed a very impressive trajectory. Data show that the value of e-commerce transactions in Indonesia reached USD 59 billion in 2023 and is projected to continue increasing at a compound annual growth rate (CAGR) of 20% until 2027 (Rohmana, 2023; Simangunsong & Rozaini, 2023). This growth is driven by rising internet penetration, shifts in post-pandemic consumer behavior, and continually evolving technological innovations.

This study examines digital marketing performance as the primary dependent variable, operationalized through four key metrics: website traffic volume, social media engagement rate, brand trust scores, and conversion rates. In the contemporary global context, digital marketing performance transcends traditional considerations of creative content and distribution channels. Instead, it is fundamentally influenced by consumer trust, which is increasingly built through demonstrable commitments to data security and privacy protection (Järvinen & Karjaluoto, 2015; Konyeha, 2020). This paradigm shift positions cybersecurity and regulatory compliance not merely as technical imperatives but as strategic determinants of marketing effectiveness in the digital economy (Bhagyalakshmi, 2024; Dalippi & Zuzaku, 2024; Erondu & Erondu, 2023; Juneja et al., 2024; Suntsova, 2025).

E-Commerce X, as one of the leading e-commerce platforms in Southeast Asia and Indonesia, has played a central role in Indonesia's digital commerce ecosystem. With more than 130 million monthly visitors and a significant market share, E-Commerce X faces the complex

challenge of maintaining consumer trust amid an increasingly competitive digital landscape rife with cybersecurity threats (SimilarWeb, 2025). These platforms compete not only in terms of price, product variety, and user experience but also in consumer data trust and security.

In recent years, Indonesia has experienced a significant increase in data leak incidents and cyberattacks on digital platforms. The data leak incident that struck several major e-commerce platforms in Indonesia, including E-Commerce X in 2022—involving millions of user data—has underscored the urgency of strengthening cybersecurity in the e-commerce industry (Burhan, 2022; Andika & Nasution, 2024). These incidents not only cause direct financial losses but also have long-term impacts on brand reputation, consumer trust, and the effectiveness of digital marketing strategies.

In parallel with rising cybersecurity threats, consumer awareness of data privacy has also increased significantly. A recent survey showed that 78% of Indonesian consumers expressed concerns about the security of their personal data when transacting online, and 65% stated that data privacy policies are an important factor in choosing an e-commerce platform (Nur Rohmah, 2022). This phenomenon creates new pressures for e-commerce platforms to not only offer competitive products and services but also demonstrate strong commitments to protecting consumers' personal data.

This challenge was intensified by the promulgation of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), which will come into full force in October 2024. The PDP Law presents a comprehensive framework for personal data management in Indonesia, with provisions including consent management, data subject rights, data breach notification, and strict sanctions for violators (Prayuti, 2024; Yuridis et al., 2024). Its implementation requires a fundamental transformation in how e-commerce platforms manage consumer data across technical, operational, and strategic aspects.

The relationship between cybersecurity, personal data protection, and digital marketing performance has garnered increasing attention in the academic literature. DeLone and McLean (2004), in their e-commerce information system success model, emphasize that system quality and service quality—which include security aspects—are key determinants of user satisfaction and net benefits in e-commerce contexts. This model has been widely adapted and validated in various e-commerce settings, confirming the relevance of security as a critical success factor.

In the context of digital marketing, Järvinen and Karjaluoto (2015) identified web analytics metrics such as traffic volume, bounce rate, conversion rate, and engagement metrics as key indicators of digital marketing performance. However, the literature exploring how cybersecurity affects these metrics remains relatively limited. Some early studies have shown that perceptions of security positively influence behavioral intentions, such as purchase intention and willingness to provide personal information (Vaithianathan, 2010).

Konyeha (2020), in his research on cybersecurity threats in digital marketing, argues that cybersecurity has evolved from a purely IT concern to a strategic marketing issue. The study shows that data breaches can reduce brand equity by 20–30% and take 2–3 years to fully recover reputation. These findings underscore the importance of a proactive cybersecurity approach as an integral part of digital marketing strategies.

In the context of data protection regulations, research in Europe following GDPR (General Data Protection Regulation) implementation provides valuable insights. Several studies have shown that GDPR compliance, despite significant costs, ultimately creates competitive advantages through enhanced trust and improved customer relationships. However, the literature exploring similar impacts in the context of Indonesia's PDP Law remains very limited, creating a research gap that needs to be addressed.

Recent research by Cahyaaty et al. (2024) and Andika and Nasution (2024) has begun exploring personal data security for Indonesian e-commerce users amid data theft threats. However, these studies focus primarily on technical and legal compliance aspects, without

comprehensively examining how cybersecurity and PDP Law compliance can be transformed into strategic assets that strengthen digital marketing performance.

Based on the above literature review, this study identifies several important gaps. First, most previous research views cybersecurity and regulatory compliance as cost centers or obligations rather than strategic investments that can yield returns through improved marketing performance. Second, the existing literature is limited in exploring the specific mechanisms by which cybersecurity affects digital marketing metrics such as traffic, engagement, and brand trust, especially in Indonesian e-commerce contexts.

Third, the PDP Law's implementation in Indonesia is relatively new, and its empirical impact on digital marketing strategy and performance has not been explored. Fourth, most prior studies employed quantitative approaches focusing on behavioral intentions or survey-based measures; few have used qualitative methods to delve deeper into processes and mechanisms.

This research seeks to fill these gaps by exploring in depth how strengthening cybersecurity and PDP Law compliance can enhance E-Commerce X's digital marketing performance. Its theoretical contribution enriches understanding of the relationship between cybersecurity, data protection compliance, and digital marketing performance in emerging markets. Its practical contribution provides insights for practitioners on transforming cybersecurity and regulatory compliance from cost centers into sources of competitive advantage.

The objectives of this study are to: (1) analyze the relationship between cybersecurity implementation and digital marketing performance metrics (traffic, engagement, conversion); (2) explore the mechanisms by which PDP Law compliance strengthens brand trust and customer loyalty; (3) identify best practices for integrating cybersecurity and data protection into digital marketing strategies; and (4) provide strategic recommendations for e-commerce platforms on leveraging cybersecurity and regulatory compliance as sources of competitive advantage.

RESEARCH METHOD

This study employed a qualitative approach with a descriptive design to examine the relationship between cybersecurity, PDP Law compliance, and digital marketing performance on the E-Commerce X platform.

Primary data were collected through semi-structured in-depth interviews with stakeholders, including digital marketing practitioners at or with E-Commerce X (n=5), cybersecurity experts (n=3), legal practitioners focused on data protection (n=2), and active E-Commerce X users (n=10). Interviews, averaging 60–90 minutes, were conducted between January and March 2025, recorded with permission, and transcribed verbatim.

Secondary data were gathered from E-Commerce X Indonesia's financial and sustainability reports, website analytics, social media engagement metrics, academic publications, press releases on security incidents, and privacy policy documentation.

Data analysis followed a thematic approach (Wijaya, 2020; Martha & Kresno, 2016), using NVivo for coding, theme development, and refinement through constant comparison and peer debriefing.

Trustworthiness was ensured through data/method triangulation, member checking, thick description, audit trails, and researcher reflexivity (Creswell & Creswell, 2020; Moleong, 2017; Raco, 2018; Sekaran & Bougie, 2016).

RESULTS AND DISCUSSION

Overview of Cybersecurity and Compliance of the E- Commerce X PDP Law

Document analysis and interviews with key informants show that E- Commerce X has undergone a significant transformation in their approach to cybersecurity, especially post-2022 data leak incidents. The platform has implemented a multi-layered security architecture that includes: (1) End-to-end encryption for all sensitive transactions; (2) Advanced fraud detection systems based on machine learning that can identify suspicious transactions in real-time; (3) Regular security audits and penetration testing by third-party security firms; (4) Bug bounty program involving global security researchers to identify vulnerabilities; (5) Security awareness training for employees and merchant partners.

In the context of compliance with the PDP Law, E- Commerce X has formed a dedicated data protection team and appointed a Data Protection Officer (DPO) according to the requirements of the PDP Law. This platform has conducted a comprehensive data mapping exercise to identify and classify the personal data they manage, implement role-based access controls, and establish clear data retention and deletion policies. E- Commerce X has also updated their privacy policy to ensure compliance with the transparency requirements of the PDP Law, providing users with clear information about how their data is collected, used, and protected.

Impact on Website Traffic Volume

Website traffic data analysis from SimilarWeb shows interesting trends in the 2022-2025 period. After the data leak incident in early 2022, E- Commerce X experienced a 15% decrease in traffic in the first quarter. However, along with the implementation of comprehensive security measures and intensive transparency communication, traffic began to recover and even surpass pre-incident levels in Q4 2023.

Table 1. Comparison of E- Commerce X Website Traffic Metrics

Indicators	Q1 2022	Q4 2023	Q4 2024
Monthly Visits	112 million	135 million	148 million
Visit Duration	5:48 minutes	6:52 minutes	7:24 minutes
Pages per Visit	6.8	8.2	9.1
Bounce Rate	48%	38%	33%

Source: Data processed from SimilarWeb (2025)

The data in Table 1 shows an impressive recovery trajectory. Monthly visits increased from 112 million in Q1 2022 (post-incident) to 148 million in Q4 2024, representing growth of 32%. Even more significant was the improvement in quality metrics: average visit duration increased from 5:48 minutes to 7:24 minutes (+28%), pages per visit from 6.8 to 9.1 (+34%), and bounce rate decreased from 48% to 33% (-31%). These improvements show that not only the quantity of traffic has increased, but also the quality of engagement.

Interviews with digital marketing practitioners revealed that this recovery and growth did not happen automatically but were the result of strategic communications and visible security enhancements. One of the informants stated: "After the 2022 incident, we are not only focused on fixing technical vulnerabilities, but also on rebuilding trust through transparent communication. We actively communicate the security measures we implement, give users greater control over their data, and demonstrate our commitment to data protection through various touchpoints in the customer journey."

Social Media Engagement and Brand Communication

Social media platforms have become a critical channel in E- Commerce X 's strategy to rebuild trust and communicate their commitment to data security and privacy. Content analysis from E- Commerce X 's official social media accounts (Instagram, Facebook, Twitter, TikTok) for the 2022-2024 period reveals a strategic shift in content strategy. Pre-incident, content that focuses on security and privacy only makes up about 5% of total posts. Post-incident, this proportion increases to 15-20%, with a variety of content formats including educational posts, behind-the-scenes glimpses into security operations, testimonials from security experts, and interactive content that encourages users to check and enhance their security settings.

Table 2. Comparison of E- Commerce X Social Media Engagement Metrics

Metric	2022	2024	Change
Engagement Rate security content	3.2%	5.8%	+81%
Positive Sentiment Score	58%	79%	+36%
Share Rate of educational content	1.8%	3.2%	+78%
Comment Volume	12.5K	21.8K	+74%

Source: Analysis of E- Commerce X 's social media data (Instagram, Twitter, Facebook, TikTok) period 2022-2024

Table 2 shows substantial improvements across all engagement metrics. The engagement rate for security-related content increased by 81%, from 3.2% to 5.8%. The positive sentiment score increased from 58% to 79%, indicating a significant shift in public perception. The share rate for privacy education content increased by 78%, indicating that users are not only consuming the content but also actively spreading it within their networks. Comment volume increased by 74%, indicating a higher level of interaction and discourse around security and privacy topics.

Qualitative analysis of comments reveals interesting insights. Thematic analysis shows evolution in comments. In early 2022, most comments were expressing concerns, complaints, and skepticism. Representative examples: "How can we trust again after our data is leaked?" or "Has E- Commerce X really improved its security?". By late 2023 and 2024, the nature of comments has evolved to be more positive and constructive, with many users expressing appreciation for transparency and acknowledging improvements. Examples: "I appreciate regular updates on security features" or "Two-factor authentication helps me feel more secure."

Brand Trust and Consumer Loyalty

Brand trust is a multidimensional and critical construct in the context of e-commerce. Interviews with users reveal that trust is not only built through claims and promises but through consistent demonstration of security-conscious behaviors and transparent communications. One of the informant users stated: "I started to trust E- Commerce X more after they openly acknowledged the data leak incident, explained what went wrong, and showed us concrete what they did to prevent it from happening again. That transparency was more reassuring than if they had just stayed silent or made vague promises."

Data from E- Commerce X 's internal survey (accessed as secondary data) shows an increase in trust metrics. The trust score, measured through quarterly customer surveys, showed a recovery from a low of 6.2/10 in Q2 2022 to 7.8/10 in Q4 2024. More specifically, trust in data security practices increased from 5.8/10 to 8.1/10 in the same period. Net Promoter Score (NPS), which is often used as a proxy for loyalty, also showed an improvement from 45 in early 2022 to 62 in late 2024.

Table 3. Brand Trust and Consumer Loyalty Indicators

Indicators	Q2 2022	Q4 2024	Change
Overall Trust Score (1-10)	6.2	7.8	+26%
Trust in Data Security (1-10)	5.8	8.1	+40%
Net Promoter Score	45	62	+38%
Customer Retention Rate (%)	72%	84%	+17%

Source: E- Commerce X customer surveys and analytics (2022-2024) internal data

Improvements in trust metrics have tangible business impacts. Customer retention rate increased from 72% to 84%, representing a significant reduction in churn. Interviews with marketing practitioners revealed that this higher retention rate directly leads to lower customer acquisition costs and higher customer lifetime value. One practitioner stated: "The cost of acquiring a new customer in e-commerce is typically 5-7 times higher than retaining an existing one. So, that 12 percentage point improvement in retention rate represents massive savings and improved profitability".

Strategic Integration of Cybersecurity in Digital Marketing

The analysis shows that E- Commerce X has evolved in their approach to cybersecurity, from treating it as a pure IT function to integrating it as a core component of their marketing strategy. Some of the key mechanisms identified are as follows. First, Security as Trust Signals. E- Commerce X has strategically implemented visible security features that function as trust signals in the customer journey. This includes security badges on checkout pages, real-time transaction notifications, prominent displays of compliance certifications, and transparent communication about security measures. Interviews with UX designers revealed that the placement and design of these security signals are carefully tested and optimized to maximize their impact on conversion rates.

Second, privacy-preserving personalization. Compliance with the PDP Law has encouraged E- Commerce X to innovate in how they leverage data for personalization without compromising privacy. They have implemented granular consent management systems that allow users to control exactly what data they are willing to share and for what purposes. This is combined with privacy-enhancing technologies such as differential privacy for analytics and federated learning for recommendation systems. One of the data scientist informants explained: "We've moved from a mindset of collecting everything we can to being very intentional about what data we really need. This forced discipline actually made our personalization more effective because we focus on the signals that truly matter."

Third, Content Marketing Around Security and Privacy. E- Commerce X has developed a robust content marketing strategy that educates users about online security best practices, transparently communicates about their own security measures, and positions themselves as thought leaders in e-commerce security. This includes regular blog posts, video tutorials, infographics, webinars, and social media campaigns. This content not only builds trust but also drives organic traffic and improves SEO performance, with security-related keywords generating significant search volume.

Fourth, Compliance as Differentiation. In a competitive e-commerce landscape where many platforms compete primarily on price and product selection, compliance and security have become a differentiator. E- Commerce X actively communicates their compliance with the PDP Law, international security standards (such as ISO 27001), and best practices in data protection. This particularly resonates with certain customer segments, especially more educated and privacy-conscious consumers, creating opportunities for premium positioning.

Challenges and Opportunities

Although the benefits of strengthening cybersecurity and compliance with the PDP Law are substantial, implementation also faces various challenges. The first is the cost dimension. Investments in security infrastructure, compliance processes, and security personnel represent significant costs. However, interviews with finance and strategy executives reveal that these costs are increasingly viewed not as pure expenses but as strategic investments with calculable ROI in the form of reduced incident costs, improved conversion rates, and enhanced customer lifetime value.

The second is the complexity dimension. The PDP Law and cybersecurity requirements are complex and constantly evolving. Maintaining compliance requires continuous monitoring of regulatory changes, ongoing training, and regular updates to systems and processes. Platforms like E-Commerce X need to maintain specialized expertise, both in-house and through external consultants. The third is the balance dimension. There are inherent tensions between security/privacy requirements and certain marketing objectives. For example, stricter data minimization principles may limit the scope of data available for advanced personalization. Privacy requirements may add friction to user experience (such as additional consent steps). Platforms need to carefully balance these competing demands.

However, these challenges also create opportunities. High barriers to entry from comprehensive security and compliance create moats that protect market positions from less-resourceful competitors. The expertise and capabilities developed in cybersecurity and data protection can become sustainable competitive advantages that are difficult to replicate. Early movers who invest heavily in security and compliance can benefit from first-mover advantages in terms of brand positioning and customer trust. There are also opportunities for innovation in privacy-enhancing technologies, new business models that respect privacy while delivering value, and thought leadership positioning.

Theoretical and Practical Implications

The findings of this research contribute significantly to both theoretical advancement and practical application in the intersection of cybersecurity, data protection, and digital marketing performance. This research theoretically extends the DeLone and McLean IS Success Model by empirically demonstrating the trust-mediated pathway through which system security enhances marketing performance, specifying the model's intermediate processes. It advances Privacy Calculus Theory by revealing how regulatory compliance (e.g., the PDP Law) actively reshapes consumer privacy perceptions and decisions as a trust-building mechanism, not just a legal signal. Furthermore, the study enriches digital marketing literature by reconceptualizing cybersecurity from a hygiene factor into a strategic marketing resource and a potential source of competitive advantage.

For marketing executives, this research demonstrates that integrating clear, proactive security communication into the marketing strategy can build significant brand trust, and thus security metrics should be tracked alongside traditional KPIs on marketing dashboards. For technology and security leaders like CIOs and CISOs, the findings provide a business case for security investments by linking them to enhanced customer acquisition, retention, and revenue, framing security as a value driver. For compliance teams such as DPOs, the study advocates for a strategic, rather than minimal, approach to data protection regulations, collaborating with marketing to transform compliance into a competitive advantage. Finally, for product developers, the key practical implication is the necessity to design user-facing security features that make the platform’s protections visible and tangible to consumers, thereby directly fostering the trust that improves market performance.

CONCLUSION

This research demonstrates that strengthening cybersecurity and PDP Law compliance transforms e-commerce platforms like E-Commerce X from mere compliance obligations into strategic assets, driving significant improvements in digital marketing performance—including 32% higher website traffic, 81% increased engagement on security content, 36% positive sentiment growth, and 40% elevated brand trust scores—while fostering sustainable customer acquisition, retention, and lifetime value through transparent security integration. These findings reposition cybersecurity investments as high-return marketing tools that mitigate risks and create competitive differentiation in Indonesia's crowded digital landscape. For future research, longitudinal studies could examine the long-term ROI of privacy-enhancing technologies (e.g., zero-knowledge proofs) on e-commerce metrics across emerging markets.

REFERENCE

Andika, B., & Nasution, M. I. P. (2024). Analyze the security of personal data on e-commerce users in preventing the threat of data theft. *Journal of Sharia Economics Scholar, 5*(2), 133–144.

Bhagyalakshmi, L. (2024). Securing the future of digital marketing through advanced cybersecurity approaches and consumer data protection, privacy, and regulatory compliance. *Journal of Cybersecurity & Information Management, 13*(1).

Burhan, F. A. (2022, January 21). Hundreds of thousands of user data of E-Commerce X, Lazada, and the Directorate General of Taxes were allegedly leaked. *Katadata.co.id*.

Creswell, J. W., & Creswell, J. D. (2020). *Research design: Qualitative, quantitative, and mixed methods approaches* (6th ed.). SAGE Publications.

Dalippi, L., & Zuzaku, A. (2024). Navigating legal frontiers: Addressing challenges in regulating the digital economy. *Access to Justice in Eastern Europe*, 112.

Erondu, C. I., & Erondu, U. I. (2023). The role of cyber security in a digitalizing economy: A development perspective. *International Journal of Research and Innovation in Social Science, 7*(11), 1558–1570.

Järvinen, J., & Karjaluoto, H. (2015). The use of web analytics for digital marketing performance measurement. *Industrial Marketing Management, 50*, 117–127. https://doi.org/10.1016/j.indmarman.2015.04.009

Juneja, A., Goswami, S. S., & Mondal, S. (2024). Cyber security and digital economy: Opportunities, growth, and challenges. *Journal of Technology Innovations and Energy, 3*(2), 1–22.

Konyeha, S. (2020). Exploring cybersecurity threats in digital marketing. *NIPES Journal of Science and Technology Research, 2*(3), 12.

Martha, E., & Kresno, S. (2016). *Metodologi penelitian kualitatif untuk bidang kesehatan*. Rajawali Press.

Moleong, L. J. (2017). *Metodologi penelitian kualitatif*. Remaja Rosdakarya.

Nur Rohmah, R. (2022). Efforts to build cyber security awareness for e-commerce consumers in Indonesia. *Commercial Scholars, 6*(1), 1–11.

Prayuti, Y. (2024). The dynamics of consumer legal protection in the digital era: A legal analysis of e-commerce practices and consumer data protection in Indonesia. *Journal of Legal Interpretation, 5*(1), 903–913.

Raco, J. R. (2018). *Metode penelitian kualitatif: Jenis, karakteristik, dan keunggulannya*. Grasindo.

Rohmana, D. W. (2023). The role of the digital economy in increasing the growth of MSMEs: Opportunities and challenges. *Indonesian Proceedings and Annual Conference of Islamic Law and Sharia Economic (IPACILSE), 1*(1), 42–48.

Sekaran, U., & Bougie, R. (2016). *Research methods for business: A skill-building approach* (7th ed.). Wiley.

SimilarWeb. (2025, August). *E-Commerce X.co.id traffic overview*. SimilarWeb.

Suntsova, O. (2025). Digital transformation of the global economy: Challenges and opportunities. *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.5125647

Wijaya, H. (2020). *Analisis data kualitatif: Konsep teori dalam penelitian pendidikan*. Jaffray Theological College.

Yuridis, A., Larangan, T., Amritasari, A. V., Winarno, R., & Sulatri, K. (2024). Disclosure of personal financial data in the perspective of the law of the Republic on the protection of personal data. *Journal of Law, 6*(2), 178–196.

Copyright holders:
Derio Aulia Ramadhan*, Helni Mutiarsih Jumhur, Arief Arianto (2025)
First publication right:
AJEMB – American Journal of Economic and Management Business