

The Relationship Between Cybersecurity and Public Trust in Digital Services: A Literature Review

**Cory Kartika Putri¹, Ahmad Nuradi², Wachid Maulana³, Andi Adri Agus⁴,
Agus Eko Setyawan⁵, Pandri Zulfikar⁶**

¹ Magister Ilmu Hukum; Syekh-Yusuf Islamic University, Tangerang - Banten;
e-mail : Cory_kartika@yahoo.com

² Magister Ilmu Hukum; Syekh-Yusuf Islamic University, Tangerang - Banten;
e-mail : ahmadnuradi17@gmail.com

³ Magister Ilmu Hukum; Syekh-Yusuf Islamic University, Tangerang - Banten;
e-mail : wachidmaulana0@gmail.com

⁴ Magister Ilmu Hukum; Syekh-Yusuf Islamic University, Tangerang - Banten;
e-mail : andiardiagus9@gmail.com

⁵ Magister Ilmu Hukum; Syekh-Yusuf Islamic University, Tangerang - Banten;
e-mail : agus.eko@gmail.com

⁶ Magister Ilmu Hukum; Syekh-Yusuf Islamic University, Tangerang - Banten;
e-mail : Pandri.zulfikar@unis.ac.id

Abstract

The rapid expansion of digital services has transformed how societies interact with public and private institutions. However, the increasing prevalence of cyber threats has raised concerns regarding data security and privacy, directly influencing public trust. This study aims to examine the relationship between cybersecurity and public trust in digital services through a systematic literature review. The findings indicate that cybersecurity effectiveness plays a critical role in shaping user confidence, particularly in contexts involving sensitive data such as digital payments and online banking. Perceived security, awareness of cyber risks, and institutional responses to cyber incidents significantly affect trust formation and retention. Moreover, trust is not solely dependent on technical security measures but also on transparency, communication, and governance frameworks. The study also highlights that cyber incidents can severely damage trust, requiring structured recovery mechanisms to rebuild confidence. Overall, the literature suggests a strong positive relationship between cybersecurity and public trust, where improved security infrastructure and user awareness enhance trust in digital

platforms. This paper contributes to the growing discourse on digital governance by emphasizing the need for integrated cybersecurity strategies to sustain public trust in digital ecosystems.

Keywords: *cybersecurity, digital trust, public trust, digital services*

INTRODUCTION

In The digital transformation of public and private services has significantly reshaped modern society, enabling efficiency, accessibility, and innovation in service delivery. Governments and organizations increasingly rely on digital platforms to provide services such as e-government, digital banking, and online commerce. However, this transformation has also exposed systems to various cybersecurity threats, including data breaches, identity theft, and cyberattacks. These risks have raised critical concerns regarding the security and reliability of digital services, ultimately influencing public trust.

Trust is a fundamental element in the adoption and continued use of digital technologies. In online environments, trust functions as a mechanism to reduce uncertainty and perceived risk, especially when users are required to share sensitive personal information (Kuen et al., 2023) . Without adequate trust, users are less likely to engage with digital services, which can hinder technological progress and digital transformation initiatives.

Cybersecurity plays a central role in shaping this trust. It encompasses the technologies, processes, and practices designed to protect systems, networks, and data from cyber threats. Studies have shown that perceived cybersecurity effectiveness significantly influences user trust in digital platforms (Gupta et al., 2025) . When users believe that systems are secure and their data is protected, they are more likely to trust and adopt digital services.

Conversely, the presence of cyber threats can negatively impact trust. For example, cyberattacks and data breaches often lead to a decline in user confidence and reduced usage of digital services (Krishna et al., 2022) . This highlights the importance of robust cybersecurity measures not only for technical protection but also for maintaining user trust. In addition, digital trust is a multidimensional concept influenced by factors such as data privacy, system reliability, and institutional integrity (Saveljeva & Volkova, 2025) . These factors collectively determine how users perceive the trustworthiness of digital systems.

This paper aims to explore the relationship between cybersecurity and public trust in digital services through a literature review approach. Specifically, it examines how cybersecurity influences trust formation, identifies key determinants of digital trust, and

351

discusses the implications for digital service providers. By synthesizing existing research, this study provides insights into how organizations can strengthen cybersecurity to enhance public trust in digital environments.

THEORETICAL REVIEW

Concept of Cybersecurity

Cybersecurity refers to the protection of digital systems, networks, and data from cyber threats such as hacking, malware, and unauthorized access. It involves a combination of technical measures, policies, and user awareness strategies aimed at ensuring data confidentiality, integrity, and availability. In cloud computing environments, cybersecurity frameworks are essential for ensuring secure data transmission and preventing breaches (Akbar et al., 2024). Cybersecurity is not only a technical issue but also a governance concern, as it involves regulatory compliance, risk management, and stakeholder collaboration. Effective cybersecurity strategies require continuous monitoring and adaptation to evolving threats.

Concept of Trust in Digital Services

Trust in digital services refers to users' confidence in the reliability, security, and integrity of digital platforms. It is a critical determinant of technology adoption and user engagement. Trust reduces perceived risks and uncertainties associated with online interactions (Lacity et al., 2024). Digital trust is multidimensional, encompassing trust in technology, service providers, and institutional frameworks. According to Saveljeva and Volkova (2025), digital trust involves confidence in people, processes, and technologies that ensure a secure digital environment.

Relationship Between Cybersecurity and Trust

The relationship between cybersecurity and trust is well established in the literature. Cybersecurity serves as a foundational factor that influences users' perceptions of safety and reliability in digital environments. Studies indicate that perceived cybersecurity effectiveness has a significant positive impact on customer trust (Gupta et al., 2025).

In digital payment systems, concerns about cybersecurity risks often deter users from adopting digital services. Cyberattacks and data breaches increase perceived risks, leading to reduced trust and lower usage rates (Krishna et al., 2022). Similarly, security risks in mobile payment applications negatively affect user trust (Putri et al., 2021). Furthermore, cybersecurity awareness and user knowledge play a significant role in shaping trust.

Individuals who perceive themselves as knowledgeable about cybersecurity may feel less vulnerable, which can influence their trust in digital platforms (De Kimpe et al., 2022) .

Trust Recovery After Cyber Incidents

Cyber incidents can severely damage public trust. However, trust can be restored through effective communication, transparency, and improved security measures. Research shows that system security and communication strategies significantly influence trust recovery in digital banking (Nurrizkiana et al., 2024) . This highlights the importance of not only preventing cyber incidents but also managing them effectively to maintain user confidence.

METHOD

This study employs a qualitative literature review approach to examine the relationship between cybersecurity and public trust in digital services. Relevant academic articles were collected from reputable journals published between 2015 and 2025. The selection criteria included peer-reviewed journal articles focusing on cybersecurity, digital trust, and technology adoption. Data were analyzed using thematic analysis to identify key patterns, relationships, and theoretical insights. The study synthesizes findings from multiple sources to provide a comprehensive understanding of how cybersecurity influences public trust in digital environments.

DISCUSSION

The findings of this study highlight a strong and consistent relationship between cybersecurity and public trust in digital services. Cybersecurity acts as a critical enabler of trust by reducing perceived risks and enhancing user confidence in digital platforms. When users believe that their data is secure, they are more likely to adopt and continue using digital services. This aligns with the broader theory of trust in digital environments, which suggests that risk mitigation is a key determinant of user acceptance (Kuen et al., 2023).

One of the key insights from the literature is that perceived cybersecurity effectiveness is more influential than actual technical security in shaping trust. Users typically lack the technical expertise to evaluate complex security systems; therefore, they rely on visible cues such as security certifications, privacy policies, and institutional reputation. This implies that organizations must not only invest in advanced cybersecurity infrastructure but also ensure that these measures are communicated clearly and transparently to users. Trust-building strategies should therefore include both technical and communicative dimensions.

Another important factor is user awareness and digital literacy. Cybersecurity awareness significantly influences how users perceive risks and trust digital platforms. Individuals with higher awareness levels are more likely to understand security protocols and engage in safer online behaviors. However, an interesting paradox emerges: users who overestimate their cybersecurity knowledge may engage in riskier behaviors, potentially increasing their vulnerability (De Kimpe et al., 2022). This finding suggests that cybersecurity education programs should focus not only on increasing knowledge but also on promoting realistic risk perceptions and responsible behavior.

The study also reveals that cybersecurity incidents have a profound negative impact on public trust. Data breaches, ransomware attacks, and unauthorized access incidents often lead to immediate declines in user confidence. In many cases, the reputational damage suffered by organizations can persist long after the technical issues have been resolved. This indicates that cybersecurity is not merely a technical issue but also a strategic and reputational concern. Organizations must therefore adopt proactive approaches to risk management, including continuous monitoring, threat intelligence, and rapid response mechanisms.

In addition, trust recovery after cybersecurity incidents is a complex and multifaceted process. The literature suggests that transparency, accountability, and effective communication are essential for rebuilding trust. Organizations that promptly disclose incidents, take responsibility, and demonstrate corrective actions are more likely to regain user confidence (Nurritziana et al., 2024). Conversely, attempts to conceal or minimize incidents can exacerbate distrust and damage long-term relationships with users.

Beyond individual organizations, the role of institutional frameworks and government regulation is also critical. Strong regulatory environments, such as data protection laws and cybersecurity standards, can enhance public trust by ensuring accountability and consistency in security practices. In emerging digital economies, including many developing countries, government involvement is particularly important in establishing baseline trust in digital systems. National cybersecurity strategies and public awareness campaigns can play a significant role in fostering a secure digital ecosystem.

Furthermore, this study finds that trust in digital services is dynamic and evolves over time. As cyber threats become more sophisticated, users' expectations regarding security also increase. Technologies such as artificial intelligence, blockchain, and biometric authentication are increasingly being integrated into cybersecurity frameworks to enhance protection. However, these technologies also introduce new challenges and uncertainties, which can affect trust if not managed properly.

Another critical dimension identified in this expanded discussion is the socio-cultural context of trust. Public trust in digital services is influenced by cultural attitudes toward technology, previous experiences with digital systems, and societal levels of institutional trust. In contexts where institutional trust is low, even strong cybersecurity measures may not be sufficient to build user confidence. Therefore, cybersecurity strategies must be adapted to local contexts, taking into account social, cultural, and behavioral factors.

Finally, the integration of cybersecurity into broader governance and service delivery models is essential. Cybersecurity should not be treated as a standalone technical function but as an integral component of digital governance. Collaborative approaches involving government, private sector, and civil society, such as the pentahelix model can enhance both cybersecurity effectiveness and public trust. This holistic approach ensures that security is embedded across all levels of digital service delivery, ultimately strengthening trust and supporting sustainable digital transformation.

CONCLUSION

This study concludes that cybersecurity has a significant and positive relationship with public trust in digital services. Effective cybersecurity measures reduce perceived risks, enhance user confidence, and encourage the adoption and continued use of digital platforms. Trust is not solely determined by technical security but is also influenced by users' perceptions, awareness, and the transparency of service providers. The literature consistently shows that cyber incidents, such as data breaches and cyberattacks, can severely undermine trust, making it difficult for organizations to recover without strategic communication and accountability. Therefore, cybersecurity must be understood as both a technical and socio-institutional issue that directly affects the sustainability of digital services.

Based on these findings, several recommendations are proposed. First, organizations should strengthen their cybersecurity infrastructure by adopting advanced technologies, continuous monitoring systems, and risk management frameworks. Second, improving transparency and communication regarding security measures is essential to build and maintain user trust. Third, governments should play an active role by establishing strong regulatory frameworks, cybersecurity standards, and public awareness programs to enhance digital trust at a national level. Fourth, digital literacy and cybersecurity awareness programs should be expanded to ensure that users can engage safely and responsibly in digital environments. Finally, a collaborative governance approach involving multiple stakeholders government, private sector, academia, and society is necessary to create a

secure and trustworthy digital ecosystem. By integrating these strategies, digital service providers can strengthen public trust and support sustainable digital transformation.

REFERENCES

- Akbar, M., Waseem, M. M., Mehanoor, S. H., & Barmavatu, P. (2024). Blockchain-based cyber-security trust model with multi-risk protection scheme for secure data transmission in cloud computing. *Cluster Computing*, 27, 9091–9105. ISSN: 1386-7857.
- De Kimpe, L., Walrave, M., Verdegem, P., & Ponnet, K. (2022). What we think we know about cybersecurity: The relationship between perceived knowledge and internet trust. *Behaviour & Information Technology*, 41(8), 1796–1808. ISSN: 0144-929X.
- Gupta, R., Pandey, P., Singh, V. K., & Sinha, K. (2025). Effectiveness of cybersecurity measures in building customer trust in digital NBFC services. *International Journal of Latest Technology in Engineering Management & Applied Science*, 14(6), 890–899. ISSN: 2278-2540.
- Kuen, L., Westmattellmann, D., Bruckes, M., & Schewe, G. (2023). Trust in online environments: A meta-analysis. *Electronic Markets*, 33(61). ISSN: 1422-8890.
- Krishna, B. M. U., Krishnan, S., & Sebastian, M. P. (2022). National cybersecurity commitment and digital payment usage. *Information Systems Frontiers*, 25(4). ISSN: 1387-3326.
- Lacity, M. C., Schuetz, S. W., Kuai, L., & Steelman, Z. R. (2024). IT's a matter of trust: Literature reviews and analyses. *Journal of Information Technology*, 40(3). ISSN: 0268-3962.
- Nurrisziana, D. D., Afifudin, A., & Alrasyid, H. (2024). Rebuilding customer trust after cyberattacks. *JEMA: Jurnal Ilmiah Bidang Akuntansi dan Manajemen*, 22(1). ISSN: 1978-1520.
- Putri, M. Z., Sutarso, Y., & Hiqmah, F. (2021). The effect of security risk on trust in mobile payment services. *Journal of Business & Banking*, 11(1). ISSN: 2088-7841.
- Saveljeva, J., & Volkova, T. (2025). A survey on digital trust: Towards a validated definition. *Digital*, 5(2), 14. ISSN: 2673-6470.
- Aljaradat, A., & Shukla, S. K. (2025). Trust and cybersecurity in digital payment adoption. *Journal of Business and Socio-economic Development*. ISSN: 2635-1692.
- Gefen, D., Karahanna, E., & Straub, D. (2003). Trust and TAM in online shopping. *MIS Quarterly*, 27(1). ISSN: 0276-7783.
- McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing trust measures for e-commerce. *Information Systems Research*, 13(3). ISSN: 1047-7047.