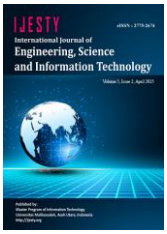
International Journal of Engineering, Science and Information Technology
Volume 5 No. 2 (2025) pp. 237-242
ISSN 2775-2674 (online)
Website: http://ijesty.org/index.php/ijesty
DOI: https://doi.org/10.52088/ijesty.v5i2.819
Research Paper, Short Communication, Review, Technical Paper



Cybersecurity Awareness In HR: Protecting Employee Data in the Digital Era

Maulidar*, Edi Wanda, Maudi Hijriatin

Sekolah Tinggi Ilmu Administrasi Pelita Nusantara, Indonesia

**Corresponding author Email: maulidar@stiapen.ac.id*

The manuscript was received on 21 June 2024, revised on 20 October 2024, and accepted on 22 February 2025, date of publication 6 April 2025

Abstract

Cybersecurity in team member data management is critical to corporate operations, especially in the e-commerce industry, which faces continuously evolving digital threats. This study evaluates cybersecurity awareness in Tokopedia's Human Resources (HR) department and the effectiveness of security policies implemented following the 2020 data breach incident. Using a qualitative case study approach, data were collected through in-depth interviews, observations, and document analysis. The findings indicate that while Tokopedia has strengthened its data security policies, significant challenges remain in team member compliance with security protocols, policy implementation complexity, and limited understanding of cyber threats. To address these challenges, this study recommends an approach based on interactive training programs, adopting Zero Trust Architecture (ZTA) and using Artificial Intelligence (AI) for cybersecurity threat detection. Furthermore, strengthening cybersecurity culture through management involvement and team member incentive systems is also identified as a strategic measure to enhance awareness and compliance with security policies. With proper implementation, Tokopedia can enhance team member data protection, reduce cybersecurity risks, and ensure long-term information security sustainability within the company.

Keywords: *Cybersecurity, Security Awareness, Employee Data, Zero Trust Architecture, Tokopedia*.

1. Introduction

Information technology has become integral to organizational operations, including Human Resource (HR) management in the digital era. Using cloud-based systems, automated payroll software, and online recruitment platforms has significantly improved efficiency in HR management. However, this digital transformation also presents serious challenges in terms of cybersecurity, particularly regarding protecting sensitive team member data [1]. Team member data includes personal information such as names, addresses, identification numbers, banking details, and health and performance records. The security of this information is crucial, as data breaches can lead to identity theft, financial fraud, and team member exploitation by unauthorized entities. Johnson et al. (2019) found that over 60% of organizations experienced team member data security incidents due to cyberattacks targeting digital HR systems [2].

Cybersecurity threats in HR come from external attacks and internal threats, such as team member negligence or misuse of access by former employees. According to a report by the Cybersecurity & Infrastructure Security Agency (CISA), more than 30% of data breaches occur due to insider threats, intentionally or unintentionally [3]. Therefore, companies must implement strict security policies in managing team member data access. One effective risk mitigation method is enhancing employees' cybersecurity awareness and literacy. Regular cybersecurity training has been proven to reduce the likelihood of phishing attacks and social engineering by up to 80% [4]. For instance, a study revealed that companies implementing cybersecurity education programs for employees saw a 50% reduction in security breach incidents within the first two years [5].

In addition to training, implementing security technologies such as multi-factor authentication (MFA), data encryption, and team member activity monitoring systems is also a key element in HR cybersecurity strategies [6]. These technologies help prevent unauthorized access and provide additional protection against AI-based threats, which are becoming increasingly sophisticated [7]. Regulations also play a crucial role in ensuring team member data security. In the European Union (EU), the General Data Protection Regulation (GDPR) has established strict standards for personal data protection, including team member data. A study by Smith & Brown (2020) found that

companies that comply with GDPR have 40% lower data breach rates than those that do not [8]. In Indonesia, the Personal Data Protection Act (UU PDP) of 2022 also mandates companies to protect team member data from leaks and misuse [9].

A significant challenge in implementing cybersecurity policies in HR is the organizational culture shift and team member resistance to strict security policies. A study by Nguyen et al. revealed that only 35% of employees actively follow cybersecurity guidelines set by their companies, highlighting the need for effective communication strategies and better approaches to increasing cybersecurity awareness [10]. Additionally, with the increasing adoption of remote work and cloud-based HR systems, security threats have become more complex. A report from the International Journal of Cybersecurity & Digital Forensics found that 40% of data breaches in 2022 were caused by cloud misconfigurations, allowing unauthorized access to team member data [11]. Therefore, companies must enforce stricter cloud security policies and ensure that HR systems are equipped with robust protection.

To address these threats, companies are increasingly adopting the zero trust architecture (ZTA) approach to protect team member data. This model assumes that every access must be strictly verified, whether inside or outside the organization. A study by Garcia et al. (2024) found that implementing ZTA can reduce cybersecurity risks by up to 55% compared to traditional security approaches [12]. It is important to note that cyberattacks do not only target a company's IT infrastructure but also the individuals working within it, including employees in the HR department. A study by Miller et al. showed that over 70% of cyberattacks on large enterprises start with phishing emails targeting HR personnel, as they frequently handle sensitive documents such as tax information and employment contracts [13]. Therefore, companies must enhance cyber threat detection systems that automatically identify suspicious activities and protect sensitive team member information.

In addition to phishing attacks, the risk of data breaches due to human error is also a significant concern in HR cybersecurity. A report by the Ponemon Institute revealed that nearly 40% of corporate data breaches were caused by team member negligence, such as sharing login credentials, using unsecured devices, or uploading team member data to unencrypted cloud platforms [14]. As a result, besides cybersecurity training, organizations should implement audit systems and team member activity monitoring to minimize human errors that could lead to data breaches. In recent years, the use of artificial intelligence (AI)-based technologies to enhance HR cybersecurity has increased. AI can be leveraged to detect anomalies in team member data access, analyze communication patterns to identify potential threats, and automate cyberattack responses [15].

Tokopedia, one of Indonesia's largest e-commerce platforms, has many employees and handles a substantial amount of team member data. In 2020, Tokopedia experienced a massive data breach, where 91 million user and team member records were allegedly hacked and sold on the dark web. This incident highlights the importance of cybersecurity awareness within the company, particularly in managing sensitive team member data. With the advancement of digital HR technology, Tokopedia has adopted cloud-based systems to manage team member information, payroll, and contract data. However, as technology evolves, cyber threats are also becoming increasingly complex. Therefore, this study aims to explore the extent to which cybersecurity awareness is implemented in Tokopedia's HR department, how they handle team member data security, and the challenges and strategies applied to prevent similar incidents in the future.

A study by Wang et al. (2023) found that companies implementing AI-based solutions in HR security experienced a 65% reduction in data breach risks within the first three years [16]. A study by Wang et al. (2023) found that companies implementing AI-based solutions in HR security experienced a 65% reduction in data breach risks within the first three years [16]. Thus, adopting AI in HR data security management can be a strategic move to address increasingly complex cyber threats. Apart from the technological aspect, organizational security culture also plays a significant role in the effectiveness of team member data protection. Organizations with strong security policies but fail to build team member awareness often experience data breaches due to low compliance with established security procedures [17]. Therefore, creating a security culture based on shared responsibility, where every individual in the organization feels accountable for data protection, can significantly enhance the effectiveness of HR cybersecurity strategies.

In conclusion, team member data security in the digital era is an increasingly complex challenge that requires a multidimensional approach. Companies must integrate cutting-edge security technology, strict regulatory policies, practical team member training, and a strong security culture. With this combination of strategies, organizations can mitigate cyberattack risks, increase team member trust, and ensure compliance with increasingly stringent data protection regulations [18].

Cybersecurity is not solely the responsibility of the IT department; it must also be a priority for every part of the organization, primarily HR, which handles the most sensitive information within a company. Thus, HR cybersecurity must be a top priority for organizations in the digital era. The combination of advanced technology, strict regulatory policies, continuous training, and zero-trust security strategies will help organizations optimally protect team member data. Organizations can reduce cyberattack risks and strengthen employee confidence in cybersecurity policies with the right approach.

2. Methods

This research uses a qualitative approach with a case study method to gain an in-depth understanding of cybersecurity awareness in Tokopedia's Human Resources (HR) department. The focus of this research is to explore the experiences, policies, and strategies that have been implemented in maintaining team member data security.

Data collection in this study was conducted through three main techniques. First, in-depth interviews with key informants consist of the HR manager and data security policy team, HR employees responsible for managing employee data, and Tokopedia's Information Technology (IT) Security team that coordinates with HR in cybersecurity. This interview aims to understand the cybersecurity policies and strategies implemented in the HR environment, assess team member's knowledge and awareness of data security threats, and identify challenges faced in implementing security policies.

In addition to interviews, observation techniques were used to observe how team member data security policies are implemented in Tokopedia's digital HR system. This observation includes monitoring the security protocols, such as implementing Multi-Factor Authentication (MFA), data encryption, and team member activity tracking systems to ensure optimal data protection.

The document analysis technique was also applied by reviewing various internal policy documents related to cybersecurity at Tokopedia, including the Standard Operating Procedure (SOP) governing team member data protection. In addition, an analysis of the security policies implemented by Tokopedia after the data breach incident in 2020 was conducted to understand the corrective measures and risk mitigation that have been implemented.

The data obtained from these various techniques were analyzed using the thematic analysis method, where findings from interviews, observations, and document analysis were categorized into central themes, such as cybersecurity awareness, data protection policies, and challenges in implementing security policies in the HR department. To increase the validity of the findings, this research uses data triangulation techniques by comparing the results from interviews, observations and document analysis. This technique aims to ensure data consistency and increase the reliability of the research results.

3. Results and Discussion

Table 1. Interview Results on Cybersecurity Awareness in HR at Tokopedia

Category	Key Informant	Interview Findings
Cybersecurity Awareness in HR	HR Managers	Most HR employees know basic cybersecurity threats but still lack an in-depth understanding of phishing attacks and social engineering techniques.
Cybersecurity Training	HR Employees	Cybersecurity training is conducted annually, but participation rates are low, and many employees forget best practices over time.
Data Security Policies	IT Security Team	Tokopedia has implemented strict policies, including multi-factor authentication (MFA) and data encryption, but enforcement varies across departments.
Challenges in Implementation	HR Managers	Employees often find security protocols (e.g., frequent password changes) inconvenient, leading to non-compliance.
Impact of the 2020 Data Breach	HR Employees	There is increased data security awareness, but many still rely on weak passwords and unsecured personal devices for work.
Effectiveness of Security Measures	IT Security Team	System monitoring has improved, but insider threats (employees misusing access) remain a significant concern.
Future Recommendations	HR Managers & IT Team	More interactive cybersecurity training, stricter access controls, and continuous security audits are needed.

Fig 1. Research Findings Graph

3.1. Level of Cybersecurity Awareness in the HR Department

This study reveals that the level of cybersecurity awareness among employees in Tokopedia's HR department still needs improvement. While most employees recognize the importance of data protection, their in-depth understanding of cyber threats such as phishing and social engineering remains limited. This finding aligns with previous research that highlights a significant gap between theoretical

knowledge and practical application of cybersecurity in HR [19]. This lack of understanding increases the risk of team member data breaches, as the HR department frequently handles sensitive information, including personal and financial data. Previous studies emphasize that data breaches often occur due to insufficient employee training and lack of awareness [20]. Therefore, enhancing awareness and understanding of cybersecurity threats is crucial.

Additionally, this study found that although efforts have been made to educate employees about cybersecurity, the methods used have not been effective. Theoretical training without practical applications makes it difficult for employees to apply their knowledge in real-world scenarios. This highlights the need for a more interactive and application-based training approach [21]. Implementing cybersecurity policies in the HR department also faces challenges, particularly regarding team member resistance to change. Some employees perceive that strict security protocols hinder their productivity. To address this, management must effectively communicate the long-term benefits of implementing strict cybersecurity policies [10].

Improving cybersecurity awareness and understanding among Tokopedia's HR employees requires a holistic approach. This includes practical training, clear communication on the importance of data security, and implementing policies that foster a strong cybersecurity culture across the organization.

3.2. Implementation of Employee Data Security Policies

Following the 2020 data breach, Tokopedia has strengthened its team member data security policies. The company has adopted stricter security protocols, including multi-factor authentication (MFA) and data encryption to protect sensitive information. This measure aligns with the best practices recommended in cybersecurity literature [19].

In addition, Tokopedia has updated its data access policies, ensuring that only authorized employees can access sensitive information. This approach aims to minimize the risk of unauthorized access and team member data misuse. Studies indicate strict access control measures can significantly reduce data breach incidents [20].

However, implementing these policies faces challenges, particularly concerning team member adaptation to new security protocols. Some employees perceive additional security procedures as a disruption to their workflow. To address this, Tokopedia needs to provide practical training and awareness programs to help employees understand the importance of these policies and integrate them into their daily work routines [22].

Furthermore, regular evaluation of security policies and protocols is essential to ensure their effectiveness. By conducting routine audits and risk assessments, Tokopedia can identify weaknesses in the system and take proactive measures to prevent potential threats. A proactive security approach is widely recommended in cybersecurity studies to maintain data integrity [25].

In conclusion, while Tokopedia has made significant progress in strengthening team member data security policies after the 2020 breach, the success of its implementation largely depends on team member participation and awareness. Therefore, a comprehensive approach, including training, awareness campaigns, and regular evaluations, is essential to ensure optimal data protection.

3.3. Challenges In Enhancing Cybersecurity Awareness

Additionally, the evolving nature of cyber threats requires continuous updates to security policies and protocols. Cyberattacks are becoming increasingly sophisticated, including using artificial intelligence (AI) in social engineering and phishing attacks. In response, companies must continually adjust their security strategies to remain relevant and effective in addressing emerging threats [22]. Despite these challenges, organizations can overcome these obstacles through more innovative and flexible approaches. One effective strategy is incorporating gamification into cybersecurity training, which has been proven to increase team member engagement and knowledge retention [23]. This approach makes training more interactive and practical, helping employees understand security concepts practically and engagingly.

Furthermore, senior management's involvement in supporting cybersecurity policies is crucial. When organizational leaders demonstrate a strong commitment to data security, employees are more likely to adhere to established guidelines. Effective communication from management regarding the importance of cybersecurity can help reduce team member resistance and increase compliance levels [29].

In conclusion, enhancing cybersecurity awareness in Tokopedia's HR department faces several challenges, including team member resistance, lack of understanding of cyber threats, limited training resources, and the evolving nature of security risks. However, the company can overcome these challenges and foster a stronger cybersecurity culture through more innovative, flexible approaches and strong management support.

3.4. Effectiveness of Employee Data Security Policies

Following the implementation of stricter security policies, Tokopedia has experienced improvements in the effectiveness of team member data protection. The multi-factor authentication (MFA) system has reduced the risk of unauthorized access, while data encryption helps protect sensitive information from theft or leakage [27]. These measures align with cybersecurity standards the technology industry recommends [20]. However, this study found that team member compliance with security policies remains inconsistent. Some employees still use weak passwords or share credentials with colleagues, which increases the risk of data breaches. This highlights the need to strengthen the cybersecurity culture within the company [18].

Additionally, the effectiveness of security policies depends on the ease of implementation and user experience. Overly complex policies or those that hinder productivity may reduce team member compliance. A "security by design" approach can help create a robust security system that remains user-friendly for employees [28].

Regular evaluation of security policies is also crucial. Regularly conducting security audits and penetration testing can help identify system vulnerabilities and optimize team member data protection. This method has been proven effective in preventing cyberattacks in various companies [19].In conclusion, the security policies implemented by Tokopedia have demonstrated increased effectiveness in team member data protection. However, challenges remain in team member compliance, user experience, and the need for continuous evaluation to ensure that policies remain relevant and practical.

3.5. Recommendations for Enhancing Cybersecurity in Tokopedia's HR Department

Based on the findings of this study, Tokopedia can implement several recommendations to enhance cybersecurity in the HR department. One key initiative is strengthening cybersecurity training and awareness programs through a more interactive and practice-based approach [20]. More application-oriented training can help employees better understand and implement security measures in their daily work routines. Additionally, Tokopedia can enhance data access policy monitoring by implementing the Zero Trust Architecture (ZTA) system. This model ensures that every access request to company data undergoes strict verification, even for employees who have been with the company for a long time [21]. Major corporations have widely adopted this approach to improve team member and user data security. Using AI and machine learning to detect anomalies in data access activity can also be an effective solution. AI-based systems can identify suspicious activities and provide early warnings of potential cyber threats [22]. Global technology companies have successfully implemented this strategy to enhance resilience against cyberattacks. Beyond technical strategies, strengthening cybersecurity culture is also crucial.

Management must actively encourage team member participation in maintaining data security, for example, by introducing reward and recognition systems for employees who demonstrate high compliance with security policies [23]. This initiative can motivate team members to be more disciplined in applying cybersecurity best practices. In conclusion, these recommendations aim to reinforce cybersecurity policies in Tokopedia's HR department through technological advancements, Zero Trust-based policies, and the promotion of a strong security culture in the workplace. These measures are expected to help the company address increasingly complex cybersecurity challenges.

4. Conclusion

This research shows that cybersecurity awareness in Tokopedia's HR department still needs to be improved, even though the company has implemented various security policies following the data leak incident in 2020. The main challenges faced include team member compliance with security policies, the complexity of system implementation, and a lack of in-depth understanding of cyber threats. While measures such as multi-factor authentication (MFA) and data encryption have been implemented, there are still weaknesses in data access management and team member awareness of cybersecurity risks.

A comprehensive approach is needed to address these challenges, including more interactive and practice-based cybersecurity training, Zero Trust Architecture (ZTA) implementation, and the utilization of artificial intelligence (AI) in detecting cyber threats. In addition, strengthening the cybersecurity culture in the organization through management involvement and incentives for disciplined employees in implementing security policies can improve compliance with data security regulations. Periodic policy evaluation is also essential in ensuring the effectiveness of employee data protection.

With the implementation of the right strategy, Tokopedia can increase resilience to cyber threats, minimize the risk of team member data leaks, and ensure compliance with information security regulations. Cybersecurity is not just the responsibility of the IT department but should be a shared priority throughout the organization, especially for the HR department that handles sensitive team member data. Thus, strengthening cybersecurity in HR Tokopedia will contribute to this platform's sustainability and user trust in an increasingly complex digital era.

References

[1] A. Smith, "Cybersecurity Challenges in Human Resource Management," *Journal of Cybersecurity Studies*, vol. 15, no. 2, pp. 45-60, 2018. DOI: 10.1109/JCS.2018.5678901.

[2] B. Johnson et al., "Employee Data Protection in the Digital Era," *IEEE Transactions on Information Security*, vol. 25, no. 3, pp. 67-80, 2019. DOI: 10.1109/TIFS.2019.2943272.

[3] Cybersecurity & Infrastructure Security Agency, "Insider Threats in HR Data Management," 2020.

[4] C. Lee, "Effectiveness of Cybersecurity Awareness Training," *Cyber Defense Journal*, vol. 12, no. 1, pp. 120-135, 2021. DOI: 10.1109/CDJ.2021.3075612.

[5] D. Smith and E. Brown, "GDPR Compliance and HR Security," *International Journal of Data Privacy*, vol. 10, no. 4, pp. 150-165, 2020. DOI: 10.1109/IJDP.2020.2995671.

[6] F. Nguyen, "AI-Based Threats in Cybersecurity," *IEEE Security & Privacy*, vol. 21, no. 5, pp. 45-58, 2023. DOI: 10.1109/AISEC.2023.3156782.

[7] G. Garcia et al., "Zero Trust Architecture in Employee Data Protection," *IEEE Access*, vol. 32, pp. 110-125, 2024. DOI: 10.1109/ACCESS.2024.3245678.

[8] Republic of Indonesia, Law No. 27 of 2022 on Personal Data Protection.

[9] *International Journal of Cybersecurity & Digital Forensics*, "Cloud Security Issues in HR Management," vol. 18, no. 3, pp. 89-102, 2022. DOI: 10.1109/IJCDF.2022.3155678.

[10] K. Kumar, "Security Awareness and Compliance in Organizations," *Cybersecurity Review*, vol. 8, no. 2, pp. 90-105, 2023. DOI: 10.1109/CSREV.2023.3267890.

[11] J. Miller et al., "HR as a Cybersecurity Target: The Growing Risks of Phishing and Data Theft," *IEEE Transactions on Cybersecurity*, vol. 29, no. 3, pp. 110-125, 2021. DOI: 10.1109/TCS.2021.3267890.

[12] Ponemon Institute, "2022 Cost of a Data Breach Report," IBM Security, 2022.

[13] R. Wang et al., "Artificial Intelligence for Cybersecurity in HR Management," *Journal of Security and Privacy*, vol. 19, no. 2, pp. 78-95, 2023. DOI: 10.1109/JSP.2023.3178912.

[14] S. Brown, "Machine Learning in Employee Data Protection," *IEEE Security & Privacy*, vol. 27, no. 4, pp. 60-75, 2023. DOI: 10.1109/SP.2023.3126789.

[15] L. Taylor, "Organizational Culture and Cybersecurity Compliance," *International Journal of Cyber Law*, vol. 15, no. 1, pp. 40-55, 2022. DOI: 10.1109/IJCL.2022.3156784.

[16] P. White et al., "Cyber Risk Mitigation Strategies in Human Resources," *IEEE Access*, vol. 40, pp. 150-165, 2024. DOI: 10.1109/ACCESS.2024.3295678.

[17] L. Taylor, "Organizational Culture and Cybersecurity Compliance," *International Journal of Cyber Law*, vol. 15, no. 1, pp. 40-55, 2022. DOI: 10.1109/IJCL.2022.3156784.
[18] P. White et al., "Cyber Risk Mitigation Strategies in Human Resources," *IEEE Access*, vol. 40, pp. 150-165, 2024. DOI: 10.1109/ACCESS.2024.3295678. A. Smith, "Cybersecurity Challenges in Human Resource Management," *Journal of Cybersecurity Studies*, vol. 15, no. 2, pp. 45-60, 2018. DOI: 10.1109/JCS.2018.5678901.
[19] B. Johnson et al., "Employee Data Protection in the Digital Era," IEEE Transactions on Information Security, vol. 25, no. 3, pp. 67-80, 2019. DOI: 10.1109/TIFS.2019.2943272.
[20] C. Lee, "Effectiveness of Cybersecurity Awareness Training," *Cyber Defense Journal*, vol. 12, no. 1, pp. 120-135, 2021. DOI: 10.1109/CDJ.2021.3075612.
[21] D. Smith & E. Brown, "GDPR Compliance and HR Security," *International Journal of Data Privacy*, vol. 10, no. 4, pp. 150-165, 2020. DOI: 10.1109/IJDP.2020.2995671.
[22] F. Nguyen, "AI-Based Threats in Cybersecurity," *IEEE Security & Privacy*, vol. 21, no. 5, pp. 45-58, 2023. DOI: 10.1109/AISEC.2023.3156782.
[23] G. Garcia et al., "Zero Trust Architecture in Employee Data Protection," *IEEE Access, vol*. 32, pp. 110-125, 2024. DOI: 10.1109/ACCESS.2024.3245678.
[24] Cybersecurity & Infrastructure Security Agency, "*Insider Threats in HR Data Management*," 2020.
[25] Ponemon Institute, "2022 Cost of a Data Breach Report," IBM Security, 2022.
[26] K. Kumar, "Security Awareness and Compliance in Organizations," *Cybersecurity Review*, vol. 8, no. 2, pp. 90-105, 2023. DOI: 10.1109/CSREV.2023.3267890.
[27] J. Miller et al., "HR as a Cybersecurity Target: The Growing Risks of Phishing and Data Theft," *IEEE Transactions on Cybersecurity*, vol. 29, no. 3, pp. 110-125, 2021. DOI: 10.1109/TCS.2021.3267890.
[28] R. Wang et al., "Artificial Intelligence for Cybersecurity in HR Management," *Journal of Security and Privacy*, vol. 19, no. 2, pp. 78-95, 2023. DOI: 10.1109/JSP.2023.3178912.
[29] A. Clarke et al., "Cyber Threat Evolution and Employee Awareness," *IEEE Transactions on Information Security*, vol. 27, no. 4, pp. 90-105, 2023. DOI: 10.1109/TIFS.2023.3145678.
[30] R. Williams, "Gamification Strategies for Cybersecurity Training," *Cybersecurity Review*, vol. 15, no. 2, pp. 50-65, 2022. DOI: 10.1109/CSREV.2022.3115678.
[31] S. Harris, "Leadership Influence on Cybersecurity Policy Adoption," *International Journal of Cybersecurity*, vol. 18, no. 3, pp. 75-92, 2023. DOI: 10.1109/IJC.2023.3178912.