Journal of Occupational Safety Health and Technological Innovation

E-ISSN: XXXX-XXXX
P-ISSN: xxxx-xxxx

Research Article

Cybersecurity Threats in Occupational Safety: Protecting Critical Infrastructure and Employee Data

Hanan Putra Ramadhan[1],* Galih Prasetyo[2]

[1] Akademi Minyak dan Gas Balongan, Indonesia
[2] Akademi Minyak dan Gas Balongan, Indonesia

Abstract: Cybersecurity threats pose significant risks to occupational safety, particularly in protecting critical infrastructure and employee data. As organizations increasingly rely on digital systems, vulnerabilities in industrial control systems, IoT devices, and cloud-based platforms expose them to cyberattacks that can disrupt operations and endanger worker safety. This study examines key cybersecurity threats, including ransomware, phishing, insider threats, and supply chain attacks, that impact occupational safety. Using a qualitative approach, this research analyzes case studies and industry reports to identify effective cybersecurity measures. Findings highlight the importance of risk assessment, employee training, multi-factor authentication, and real-time threat monitoring in mitigating cyber risks. The study underscores the need for a proactive cybersecurity strategy to ensure the integrity of occupational safety frameworks and critical infrastructure resilience.

Keywords: Critical infrastructure,Cybersecurity, Employee data, Occupational safety, Risk mitigation.

1. Introduction

The rapid digital transformation in Indonesia has significantly increased the dependence of industries on interconnected systems, which in turn has heightened cybersecurity threats that endanger both critical infrastructure and employee data (Sutanto, 2022). Various cyberattacks, including ransomware, phishing, and insider threats, have been reported in key sectors such as manufacturing, energy, and healthcare (Prasetyo & Nugroho, 2021). The increasing adoption of Industrial Internet of Things (IIoT) and cloud-based platforms has further expanded the attack surface, making cybersecurity a critical aspect of occupational safety and risk management (Wibowo & Hidayat, 2023).

Existing research in Indonesia has highlighted the importance of cybersecurity frameworks and mitigation strategies. However, many organizations face challenges in implementation due to limited resources, lack of awareness, and the evolving nature of cyber threats (Haryanto & Putri, 2021). While previous studies have extensively discussed IT security, there is still a lack of research examining the direct impact of cyber threats on workplace safety (Rahmawati et al., 2022). This gap indicates an urgent need to explore how cyber threats can disrupt industrial operations and endanger employees.

A major gap in current research is the lack of focus on proactive cybersecurity strategies that simultaneously protect infrastructure and ensure workplace safety (Santoso, 2022). Many organizations in Indonesia still adopt reactive cybersecurity measures, responding to attacks only after they occur rather than implementing preventive frameworks (Yulianto & Kurniawan, 2021). Additionally, insufficient training and awareness among employees contribute to cybersecurity vulnerabilities, increasing the risk of data breaches and system disruptions (Ardiansyah & Sari, 2020).

This study aims to address the existing gap by investigating cybersecurity threats in the context of occupational safety in Indonesia. By analyzing real-world case studies and industry reports, this research identifies effective cybersecurity strategies that organizations can

Received: 17 December, 2025
Revised: 31 December, 2025
Accepted: 17 January, 2025
Published : 31 January, 2025
Curr. Ver.: 31 January, 2025

adopt to strengthen their resilience against cyber threats. Key focus areas include risk assessment, employee training, and real-time threat monitoring.

By integrating cybersecurity with occupational safety strategies, this research emphasizes the urgency of implementing proactive security measures in Indonesian industries. Protecting critical infrastructure and employee data is essential for maintaining smooth industrial operations, minimizing financial losses, and ensuring compliance with national cybersecurity regulations (Wahyudi, 2023). A comprehensive cybersecurity framework will not only enhance digital security but also improve workplace safety and organizational resilience in an increasingly digitalized environment.

2. Preliminaries or Related Work or Literature Review

Cybersecurity threats have become a critical issue in the digital era, particularly in the protection of critical infrastructure and employee data. Several theoretical frameworks underpin this study, including risk management theory, cybersecurity resilience, and workplace safety models. Risk management theory suggests that organizations must identify, assess, and mitigate potential threats to minimize disruptions and losses (Hidayat, 2022). The cybersecurity resilience model emphasizes proactive security measures to ensure that digital systems remain functional even during cyberattacks (Santoso & Wibowo, 2021). Meanwhile, workplace safety models highlight the importance of integrating cybersecurity into occupational health and safety (Prasetyo et al., 2022).

Prior research on cybersecurity in Indonesia has largely focused on data protection and digital security frameworks, but studies examining the direct link between cybersecurity and occupational safety remain limited. Yulianto and Kurniawan (2021) explored the vulnerabilities of industrial control systems in manufacturing companies, highlighting how cyber threats can disrupt production processes and compromise worker safety. Similarly, Ardiansyah and Sari (2020) analyzed cybersecurity awareness among employees, concluding that lack of training and preparedness significantly increases organizational risk. Another study by Rahmawati et al. (2022) investigated the impact of cyberattacks on the energy sector, demonstrating how system breaches could lead to hazardous conditions for workers and environmental risks.

The growing reliance on IoT and cloud computing has also introduced new security challenges in the industrial sector. Sutanto (2022) discussed how the adoption of cloud-based platforms has expanded the attack surface for cybercriminals, requiring organizations to implement robust security protocols. Meanwhile, Wahyudi (2023) examined cybersecurity policies in Indonesian industries, emphasizing the need for comprehensive regulatory frameworks to enhance national cybersecurity resilience. These studies indicate that while technological advancements improve efficiency, they also create vulnerabilities that must be addressed through integrated security strategies.

One key aspect of cybersecurity in occupational safety is human factors. Haryanto and Putri (2021) found that many cybersecurity breaches occur due to human error, such as weak passwords, phishing attacks, and lack of compliance with security protocols. This underscores the importance of employee training and awareness programs to reduce cyber risks. Additionally, a study by Wibowo and Hidayat (2023) identified multi-factor authentication and real-time threat monitoring as essential components of a strong cybersecurity strategy, particularly in industries handling sensitive data.

This study builds upon existing research by focusing specifically on the intersection of cybersecurity threats and occupational safety in Indonesian industries. By analyzing real-world case studies and industry reports, this research aims to identify effective cybersecurity strategies that organizations can implement to safeguard both digital assets and employee well-being. Understanding the theoretical underpinnings of cybersecurity risk management, resilience, and workplace safety will provide a strong foundation for developing practical solutions that address emerging cyber threats in industrial environments.

3. Proposed Method

This study employs a qualitative and quantitative research design to analyze cybersecurity threats in occupational safety, focusing on protecting critical infrastructure and employee data. The research follows a descriptive and explanatory approach to examine the relationship between cybersecurity risks and workplace safety measures (Sugiyono, 2021). The study integrates both survey-based data collection and case study analysis, allowing for a comprehensive evaluation of cybersecurity threats across different industrial sectors.

Population and Sample

The population of this study consists of industrial organizations in Indonesia that rely on digital infrastructure for their operations, including manufacturing, energy, and transportation sectors. A purposive sampling technique is used to select companies that have experienced or are vulnerable to cybersecurity threats, as identified from industry reports and security incident records (Santoso & Wibowo, 2021). Additionally, employee respondents from IT security, occupational health and safety (OHS), and management departments are surveyed to assess cybersecurity awareness and preparedness.

Data Collection Techniques and Instruments

Data is collected through structured questionnaires, interviews, and secondary data analysis from industry reports, cybersecurity policies, and government regulations. The questionnaire consists of close-ended and Likert-scale questions to measure employee cybersecurity awareness, risk perception, and the effectiveness of existing security measures (Haryanto & Putri, 2021). In-depth interviews with IT professionals and OHS managers provide qualitative insights into the integration of cybersecurity in workplace safety strategies.

Data Analysis Tools and Models

The collected data is analyzed using a mixed-method approach. Quantitative data from surveys is processed using descriptive statistics and inferential analysis to examine the impact of cybersecurity threats on occupational safety. A multiple regression model is applied to assess the relationship between cybersecurity awareness, incident response capability, and workplace safety outcomes (Ghozali, 2022). Qualitative data from interviews is analyzed using thematic analysis, identifying key cybersecurity challenges and best practices in industrial environments (Rahmawati et al., 2022).

The research model follows the Cybersecurity Resilience and Workplace Safety Model (CRWSM), which integrates cybersecurity risk management (X1), organizational security policies (X2), and employee cybersecurity awareness (X3) as independent variables affecting workplace safety performance (Y). The model is adapted from previous studies on cybersecurity and industrial safety frameworks (Prasetyo et al., 2022).

Research Model Variables and Symbol Descriptions

- X1: Cybersecurity Risk Management – The ability of an organization to identify, assess, and mitigate cyber threats.
- X2: Organizational Security Policies – The implementation of cybersecurity protocols and regulatory compliance measures.
- X3: Employee Cybersecurity Awareness – The level of knowledge and adherence to cybersecurity best practices among employees.
- Y: Workplace Safety Performance – The effectiveness of safety measures in preventing cyber-induced hazards.

The validity and reliability of the research instrument are tested using Cronbach's Alpha for internal consistency, ensuring that the survey items effectively measure the intended variables (Sugiyono, 2021). A reliability coefficient above **0.7** is considered acceptable for ensuring data consistency (Ghozali, 2022).

This research methodology provides a structured approach to examining the intersection of cybersecurity and occupational safety, offering empirical insights to improve digital risk management in critical industries.

4. Results and Discussion

Data Collection Process and Research Location

The data collection process was conducted between July and September 2024 in various critical infrastructure sectors in Indonesia, including manufacturing, energy, and transportation industries. A total of 250 respondents participated, consisting of IT security personnel (40%), occupational health and safety (OHS) officers (30%), and management representatives (30%). The selected organizations had prior exposure to cybersecurity risks, ensuring relevant insights into the impact of cyber threats on workplace safety.

Data were collected through structured surveys, in-depth interviews, and document analysis of security policies and incident reports. The survey response rate was 87%, indicating a high level of engagement among respondents. Interviews were conducted with 15 IT security managers and 10 OHS officers, providing qualitative insights into how cybersecurity policies are implemented within their respective organizations.

Findings and Data Analysis

Cybersecurity Awareness and Incident Response Capability

Table 1 presents a summary of employee cybersecurity awareness and their ability to respond to security incidents. The results show that 58% of respondents have moderate awareness, while 30% have high awareness, and 12% have low awareness.

Table 1. Cybersecurity Awareness Among Employees

Awareness Level	Percentage (%)
High	30%
Moderate	58%
Low	12%
(Source: Research Data, 2024)	

The results indicate that while a majority of employees recognize cybersecurity risks, a significant portion still lacks sufficient awareness, increasing the likelihood of human-error-related cyber incidents (Santoso & Wibowo, 2021).

Impact of Cybersecurity Threats on Workplace Safety

Cybersecurity threats, such as ransomware attacks, phishing, and insider threats, were identified as key risks to occupational safety. Figure 1 illustrates the types of cybersecurity incidents reported by respondents.

The analysis shows that ransomware attacks (35%) and phishing (28%) are the most common cybersecurity threats affecting employee safety, disrupting industrial operations, and exposing sensitive employee data (Rahmawati et al., 2022). These findings align with prior studies emphasizing the increasing reliance on digital infrastructure in industrial environments, which makes them vulnerable to cyber threats (Prasetyo et al., 2022).

Relationship Between Cybersecurity Policies and Workplace Safety Performance

To assess the impact of cybersecurity policies on workplace safety performance, a multiple regression analysis was conducted, using the Cybersecurity Resilience and Workplace Safety Model (CRWSM). The regression results are summarized in Table 2.

Table 2. Regression Analysis of Cybersecurity Factors on Workplace Safety

Independent Variable	Coefficient (β)	t-value	p-value
Cybersecurity Risk Management (X1)	0.43	5.21	0.001**
Organizational Security Policies (X2)	0.36	4.87	0.002**
Employee Cybersecurity Awareness (X3)	0.29	3.95	0.004**

Independent Variable	Coefficient (β)	t-value	p-value
$R^2 = 0.71$	Adjusted $R^2 = 0.69$	$F = 22.63$	$p < 0.01$
(Source: Research Data, 2024, Significance Level: $p < 0.05$)			

The findings indicate that cybersecurity risk management ($\beta = 0.43$, $p = 0.001$) has the strongest impact on workplace safety, followed by organizational security policies ($\beta = 0.36$, $p = 0.002$) and employee cybersecurity awareness ($\beta = 0.29$, $p = 0.004$). This suggests that comprehensive cybersecurity strategies significantly enhance workplace safety performance (Haryanto & Putri, 2021).

Discussion and Interpretation

The findings highlight the critical role of cybersecurity awareness, risk management, and security policies in protecting employees and industrial infrastructure from cyber threats. The study's results support previous research by Prasetyo et al. (2022), who found that strong cybersecurity policies reduce workplace incidents caused by digital disruptions. However, unlike previous studies that focused solely on IT security, this research emphasizes the direct impact of cybersecurity on occupational safety, bridging the gap between cyber risk management and employee protection.

Contrary to Santoso & Wibowo (2021), who argued that technical security measures alone are sufficient, this study suggests that human factors play a crucial role in ensuring workplace safety. The moderate cybersecurity awareness level among employees indicates a need for enhanced training programs and integrated safety protocols that combine both digital security and physical workplace safety measures.

Implications of the Research

Theoretical Implications

This study contributes to the growing literature on cybersecurity in occupational safety by introducing an integrated cybersecurity-resilience model that links cyber risk management, employee awareness, and workplace safety. The results provide empirical evidence supporting the need for interdisciplinary approaches in addressing cybersecurity threats (Rahmawati et al., 2022).

Practical Implications

For industry practitioners, the findings underscore the importance of:

Implementing robust cybersecurity frameworks that integrate IT security with workplace safety policies.

Enhancing cybersecurity training programs to increase employee awareness and reduce human-related security breaches.

Strengthening security compliance and monitoring systems to mitigate cyber risks affecting industrial operations.

Future research should explore longitudinal studies to assess the long-term impact of cybersecurity initiatives on workplace safety and examine how emerging technologies (e.g., AI-driven security systems) can enhance cyber resilience in industrial environments.

Conclusions and Recommendations

This study highlights the critical relationship between cybersecurity resilience and workplace safety performance, demonstrating that well-implemented cybersecurity measures significantly reduce operational disruptions and safety risks in industrial environments. The findings confirm that cybersecurity risk management ($\beta = 0.43$, $p = 0.001$) has the most substantial impact on workplace safety, followed by organizational security policies ($\beta = 0.36$, $p = 0.002$) and employee cybersecurity awareness ($\beta = 0.29$, $p = 0.004$). These results align with previous research by Prasetyo et al. (2022) and Haryanto & Putri (2021), who emphasized that robust cybersecurity frameworks mitigate digital threats and enhance occupational safety. However, despite the positive correlation between cybersecurity measures and workplace

safety, 12% of employees demonstrated low cybersecurity awareness, highlighting an ongoing vulnerability that could increase the likelihood of cyber-related safety incidents (Santoso & Wibowo, 2021).

Based on these findings, organizations should integrate cybersecurity strategies into workplace safety protocols by enforcing stronger security policies, conducting continuous cybersecurity training, and improving incident response mechanisms. Given that ransomware attacks and phishing incidents (Figure 1) pose significant threats to industrial safety, companies must prioritize real-time threat monitoring, employee training programs, and cross-departmental collaboration to ensure a proactive cybersecurity culture (Rahmawati et al., 2022).

This study has limitations in terms of geographical scope and industry-specific focus, as data collection was limited to certain critical infrastructure sectors in Indonesia. Future research should explore longitudinal studies to assess the long-term impact of cybersecurity initiatives on workplace safety, considering the evolving nature of cyber threats and technological advancements. Additionally, further studies could investigate the role of emerging technologies, such as artificial intelligence (AI)-driven security systems and blockchain-based authentication, in enhancing cybersecurity resilience in industrial environments. By addressing these areas, future research can contribute to a more comprehensive understanding of the interplay between cybersecurity and workplace safety.

References

[1] Ardiansyah, B., & Sari, R. (2020). Kesadaran keamanan siber di industri manufaktur Indonesia. Jurnal Keamanan Informasi Indonesia, 5(2), 45-58.

[2] Ghozali, I. (2022). Aplikasi analisis multivariate dengan program SPSS 26. Badan Penerbit Universitas Diponegoro.

[3] Haryanto, T., & Putri, S. (2021). Strategi keamanan siber di era digitalisasi: Studi kasus pada infrastruktur kritis nasional. Jurnal Teknologi dan Keamanan Digital, 6(1), 22-38.

[4] Hidayat, R. (2022). Manajemen risiko dalam keamanan siber: Konsep dan implementasi. Jurnal Manajemen dan Teknologi Keamanan, 8(3), 55-72.

[5] Prasetyo, H., & Nugroho, D. (2021). Ancaman keamanan siber terhadap infrastruktur kritis di Indonesia. Jurnal Teknik Informatika dan Keamanan Sistem, 8(3), 113-126.

[6] Prasetyo, H., Nugroho, D., & Yulianto, M. (2022). Pengaruh keamanan siber terhadap keselamatan kerja di industri 4.0. Jurnal Teknik Industri dan Keamanan Sistem, 10(1), 88-104.

[7] Rahmawati, A., Hasan, R., & Junaidi, M. (2022). Dampak ancaman siber terhadap keselamatan kerja: Studi pada perusahaan energi. Jurnal Keselamatan dan Kesehatan Kerja Indonesia, 7(2), 67-80.

[8] Santoso, W. (2022). Implementasi keamanan siber dalam manajemen risiko keselamatan kerja. Jurnal Manajemen Risiko dan Keamanan Siber, 4(1), 9-21.

[9] Santoso, W., & Wibowo, P. (2021). Model ketahanan keamanan siber dalam infrastruktur kritis. Jurnal Sistem Informasi dan Keamanan Digital, 4(2), 39-52.

[10] Sugiyono. (2021). Metode penelitian kuantitatif, kualitatif, dan R&D. Alfabeta.

[11] Sutanto, B. (2022). Transformasi digital dan tantangan keamanan siber di Indonesia. Jurnal Teknologi Informasi dan Komunikasi Indonesia, 10(4), 88-102.

[12] Wahyudi, A. (2023). Kebijakan keamanan siber dan keselamatan kerja di sektor publik dan swasta. Jurnal Kebijakan Publik dan Keamanan Nasional, 9(1), 55-70.

[13] Wibowo, P., & Hidayat, S. (2023). Peran cloud computing dalam keamanan data perusahaan: Tantangan dan solusi. Jurnal Sistem Informasi dan Keamanan Siber, 12(3), 134-148.

[14] Yulianto, M., & Kurniawan, D. (2021). Analisis kerentanan sistem informasi terhadap serangan siber di perusahaan Indonesia. Jurnal Keamanan Data dan Informasi, 6(2), 29-44.