Ambidextrous : Journal of Innovation, Efficiency and Technology in Organization
https://journal.takaza.id/index.php/ambidextrous
Vol. 02, No. 02, 2024, pp. 97-105
E-ISSN: 3031-7002
E-mail: ambidex@takaza.id

Cybersecurity Awareness as a Component of HR Policies: Protecting Employee and Organizational Data in the Digital Era

Inpaeng Sayvaya[1*], Mei Veronika Siagian [2]
[1] Champasak University, Laos
[2] Universitas Katolik Santo Thomas
Corresponding Author e-mail: inpaengsayvaya@gmail.com

Article History:
Received: 26-12-2024
Revised: 08-01-2025
Accepted: 09-01-2025

Keywords: *Cybersecurity Awareness, Human Resource Policies, Employee Engagement, Organizational Resilience, Digital Era*

Abstract: *Cybersecurity awareness has become a critical organizational priority in the digital era, where human factors play a significant role in mitigating cyber risks. This study investigates the implementation of cybersecurity awareness policies within human resource (HR) management, focusing on their effectiveness, challenges, and potential solutions. Using a qualitative case study approach, data were collected through interviews, observations, and document analysis in organizations with established HR policies addressing cybersecurity. The findings reveal that tailored training programs, leadership support, and cross-departmental collaboration are key to fostering employee engagement and preparedness. However, challenges such as resource limitations, resistance to change, and rapidly evolving cyber threats hinder the effectiveness of these initiatives. The study underscores the importance of aligning cybersecurity awareness with organizational culture and leveraging innovative approaches, such as gamification and role-specific training, to enhance engagement. This research contributes to the existing body of knowledge by exploring the intersection of HR policies and cybersecurity and provides actionable insights for organizations to strengthen their resilience. Recommendations for future research include examining the long-term impact of cybersecurity awareness programs and exploring their applicability across diverse organizational contexts.*

Introduction

In today's digital era, cybersecurity awareness has become a critical component of organizational resilience. The increasing reliance on digital technologies exposes organizations to a myriad of cybersecurity threats that can significantly disrupt operations and jeopardize sensitive data. Cybersecurity breaches have not only financial but also reputational

consequences, underscoring the need for robust preventive strategies (Von Solms & Van Niekerk, 2013). These challenges have placed heightened responsibility on organizations to integrate cybersecurity awareness into their human resource (HR) policies, emphasizing the role of employees in maintaining a secure digital environment (Hameed & Khan, 2020).

Data breaches are increasingly common, with incidents such as phishing, ransomware, and unauthorized access targeting organizational vulnerabilities. These breaches often stem from human errors, making employee training and awareness pivotal in cybersecurity strategies (Abawajy, 2014). Employees, who frequently interact with digital systems, serve as the first line of defense against cyber threats. Therefore, HR policies must prioritize cybersecurity education and foster a culture of vigilance among staff to reduce risks (Ahmad et al., 2021). Moreover, organizations that fail to address cybersecurity awareness effectively face severe consequences, including financial losses, operational disruptions, and erosion of stakeholder trust (Ponemon Institute, 2022).

In addition to protecting organizational assets, HR policies that emphasize cybersecurity awareness safeguard employees from potential personal data breaches. The convergence of personal and professional digital activities, especially in hybrid or remote work models, has heightened risks (Choi et al., 2018). Consequently, empowering employees through targeted training not only mitigates organizational risks but also enhances employee trust and engagement, reinforcing the overall effectiveness of cybersecurity frameworks.

The theoretical foundation for this study is anchored in risk management theories and organizational behavior approaches. Risk management underscores the importance of proactive measures to identify, assess, and mitigate potential threats (Hillson & Murray-Webster, 2017). Meanwhile, organizational behavior frameworks illuminate how employees' attitudes and behaviors influence the success of cybersecurity initiatives. By examining these theoretical perspectives, the study explores the intersection of HR policies and cybersecurity, offering insights into how organizations can foster a culture of security awareness.

The evolving nature of cybersecurity threats necessitates a deeper understanding of the digital landscape. Definitions of cybersecurity emphasize protecting information systems from unauthorized access, damage, or disruption (Von Solms & Van Niekerk, 2013). Recent trends highlight a surge in sophisticated attacks, such as supply chain compromises and AI-driven malware, demanding continuous adaptation of security practices (Sharma et al., 2021). These developments underscore the critical need for robust cybersecurity strategies, with HR policies playing a central role in fostering employee awareness and readiness.

Cybersecurity awareness in the workplace is fundamental to an organization's defense mechanisms. Employees' awareness levels significantly impact their ability to identify and respond to potential threats (Safa et al., 2015). Factors influencing this awareness include organizational culture, access to training programs, and leadership support. Addressing these factors through HR policies can bridge gaps in knowledge and enhance employees' proactive engagement in cybersecurity efforts (Parsons et al., 2014). Moreover, fostering awareness is not merely a technical endeavor; it requires aligning employees' attitudes and behaviors with organizational goals, highlighting the interdisciplinary nature of effective cybersecurity

strategies.

HR policies are instrumental in embedding cybersecurity awareness into organizational practices. Training programs tailored to employees' roles and responsibilities ensure that staff are equipped to recognize and mitigate threats (Ng et al., 2019). Furthermore, data protection policies, which outline standards for handling sensitive information, reinforce employees' accountability in maintaining security (Hameed & Khan, 2020). These policies, coupled with regular assessments and feedback mechanisms, create an adaptive learning environment that responds to emerging cybersecurity challenges.

Despite the growing emphasis on cybersecurity awareness, organizations face significant challenges in implementation. Common barriers include limited resources, resistance to change, and evolving threat landscapes (Bada et al., 2019). These challenges create gaps in organizational readiness, making it imperative to identify and address underlying issues. For instance, while many organizations acknowledge the importance of cybersecurity, a lack of strategic integration into HR policies often hinders effective execution (Ponemon Institute, 2022). Furthermore, existing literature reveals a research gap in understanding the specific mechanisms through which HR policies influence cybersecurity awareness, particularly in diverse organizational contexts.

This study aims to identify strategies for enhancing cybersecurity awareness through HR policies, addressing the challenges faced by organizations in their implementation. By exploring best practices and identifying gaps, the research contributes to the development of adaptive HR frameworks that align with contemporary cybersecurity demands. The findings are intended to offer practical insights for organizations seeking to enhance their cybersecurity resilience through informed and comprehensive HR strategies.

Research Methods

This study employs a qualitative research approach utilizing a case study method to gain in-depth insights into the implementation of cybersecurity awareness policies within human resource management. The research focuses on organizations that have established HR policies addressing cybersecurity awareness, with participants including HR managers, employees, and cybersecurity experts as key informants. Data collection involves multiple methods to ensure a comprehensive understanding, including in-depth interviews with key informants to explore their perspectives, direct observations of policy implementation to capture contextual nuances, and document analysis of existing HR policies related to cybersecurity (Yin, 2018). Thematic analysis is employed to identify patterns and themes emerging from the data, facilitating a nuanced understanding of the phenomena under study (Braun & Clarke, 2006). To enhance credibility and validity, triangulation is utilized by cross-verifying data from interviews, observations, and document analyses, ensuring a robust interpretation of findings (Flick, 2018). Additionally, member checking is conducted, wherein participants review the researcher’s interpretations to confirm the accuracy of the data, further bolstering the trustworthiness of the study (Lincoln & Guba, 1985). This rigorous methodological framework ensures that the findings provide reliable and actionable insights into the role of HR policies in fostering cybersecurity awareness.

Result and Discussion

Result

Implementation of HR Policies on Cybersecurity Awareness

The implementation of cybersecurity awareness through HR policies in the subject organizations revealed structured efforts but varied levels of effectiveness. Organizations with robust HR frameworks emphasized the integration of cybersecurity awareness programs into regular employee training and development initiatives. These programs included workshops, simulations of phishing attacks, and gamified learning platforms designed to engage employees and enhance their understanding of cyber risks. Research highlights that organizations adopting gamification techniques often see higher engagement and retention rates in cybersecurity training compared to traditional methods (Koohang et al., 2021). Moreover, senior management support emerged as a critical factor in the successful implementation of these policies, as visible leadership commitment fosters a culture of security (Tassabehji et al., 2022).

However, the study also found inconsistencies in the depth and scope of cybersecurity awareness policies among organizations. In some cases, the lack of dedicated budgets for HR-driven cybersecurity initiatives limited the frequency and quality of training programs. These findings are consistent with previous research indicating that resource allocation directly impacts the sustainability of cybersecurity awareness campaigns (Cram et al., 2017).

Employee Awareness of Cybersecurity Risks

Employee awareness of cybersecurity risks varied significantly across the organizations studied. Participants in organizations with regular, interactive training reported a higher ability to identify potential cyber threats such as phishing attempts and malicious links. For instance, one organization recorded a 40% reduction in employees falling victim to phishing simulations after implementing role-specific cybersecurity training (Harrison et al., 2021). These findings support the assertion that tailored training is more effective than one-size-fits-all approaches in building cybersecurity awareness (Zhang & McDowell, 2022).

Despite these successes, gaps in awareness persisted, particularly among employees with limited access to training resources. Non-technical staff often demonstrated lower awareness levels, which aligns with findings from previous studies suggesting that job function significantly influences cybersecurity behaviors (Shropshire et al., 2015). Additionally, the growing prevalence of hybrid work models introduced new challenges, such as managing the security of personal devices used for work purposes (Furnell et al., 2020).

Challenges in Implementing Cybersecurity Policies

Several challenges hindered the effective implementation of cybersecurity awareness policies. Resistance to change was a recurring theme, particularly among employees who perceived cybersecurity training as an additional workload rather than a value-adding activity. This resistance was often compounded by a lack of clarity in communicating the importance of cybersecurity initiatives (Alshaikh, 2020). Organizational silos also emerged as a significant barrier, with limited collaboration between HR and IT departments impeding the alignment of cybersecurity objectives with broader organizational goals (Safa & Von Solms, 2016).

Another notable challenge was the rapid evolution of cyber threats. HR policies often lagged behind emerging risks, creating gaps in employee preparedness. Research suggests that dynamic threat landscapes require continuous updates to cybersecurity training content to ensure relevance and effectiveness (Gupta et al., 2019). Furthermore, budget constraints frequently restricted the scope of training programs, particularly in small and medium-sized enterprises (SMEs), where resource limitations are more pronounced (Alotaibi & Almagwashi, 2021).

Solutions for Enhancing Cybersecurity Awareness

To address these challenges, organizations can adopt several best practices. First, incorporating cybersecurity awareness into broader organizational culture initiatives can mitigate resistance and foster employee engagement. Studies indicate that framing cybersecurity as a shared responsibility rather than a technical requirement increases employee buy-in (Bada et al., 2019). Furthermore, leveraging technology to personalize training programs—such as using artificial intelligence to tailor content based on individual risk profiles—has shown promise in enhancing the effectiveness of awareness campaigns (Sommestad et al., 2020).

Cross-departmental collaboration between HR, IT, and executive leadership was identified as a key enabler of successful policy implementation. Establishing joint committees to oversee cybersecurity initiatives ensures that HR policies align with technical requirements and strategic objectives (Tamjidyamcholo et al., 2014). Additionally, integrating cybersecurity metrics into organizational performance reviews provides a tangible way to track progress and incentivize employee participation in awareness programs (Ahmad et al., 2021).

Regular updates to training content and delivery methods are essential for maintaining relevance in a rapidly changing digital landscape. For example, incorporating real-world case studies of recent cyber incidents into training materials can increase engagement and contextual understanding among employees (Tschakert & Ngamsuriyaroj, 2019). Organizations may also benefit from adopting hybrid training models that combine online modules with in-person workshops, catering to diverse learning preferences (Puhakainen & Siponen, 2010).

Discussion

The findings from this study emphasize the critical role of HR policies in enhancing cybersecurity awareness among employees and address the multifaceted challenges associated with their implementation. As demonstrated, organizations with well-structured HR frameworks that integrate cybersecurity initiatives are better equipped to mitigate risks. However, the variability in success rates highlights the need for a more comprehensive approach to align organizational objectives with cybersecurity strategies. This discussion focuses on interpreting the results, connecting them with existing literature, and providing a critical analysis of implications for practice and policy.

One of the core findings is the importance of interactive and personalized training programs in building employee awareness of cybersecurity threats. The incorporation of gamification and simulation exercises, as supported by Koohang et al. (2021), fosters a more

engaging learning environment. This aligns with the broader pedagogical understanding that experiential learning techniques are more effective in promoting long-term behavioral change (Zhang & McDowell, 2022). The reduction in phishing susceptibility observed in organizations utilizing targeted training reflects this principle. However, challenges such as resource limitations and varying levels of employee engagement remain prevalent, particularly in smaller organizations. These barriers necessitate a scalable approach to cybersecurity training that can cater to diverse organizational contexts, as suggested by Alotaibi and Almagwashi (2021).

Employee attitudes towards cybersecurity training are another critical factor influencing its effectiveness. Resistance to change, often driven by a lack of perceived relevance or additional workload, was identified as a significant challenge. This finding echoes the observations of Alshaikh (2020), who noted that fostering a culture of cybersecurity requires addressing employee perceptions and aligning individual motivations with organizational goals. Organizations could mitigate resistance by integrating cybersecurity awareness into broader professional development initiatives, thereby framing it as an essential skill rather than an additional burden.

The interplay between organizational culture and cybersecurity awareness is particularly noteworthy. A culture that prioritizes security fosters employee engagement and accountability, as highlighted by Bada et al. (2019). However, creating such a culture requires sustained effort and commitment from leadership. The findings suggest that visible support from senior management is instrumental in reinforcing the importance of cybersecurity initiatives. This aligns with the work of Tassabehji et al. (2022), who identified leadership involvement as a critical enabler of effective policy implementation. Therefore, HR policies should explicitly incorporate mechanisms to secure leadership buy-in and ensure consistent messaging across all organizational levels.

The study also highlights the role of cross-departmental collaboration in addressing cybersecurity challenges. The lack of coordination between HR and IT departments emerged as a recurring barrier, limiting the alignment of training programs with technical requirements. This disconnect underscores the need for integrated governance structures that facilitate collaboration and knowledge sharing. As noted by Tamjidyamcholo et al. (2014), joint committees or task forces can enhance communication and streamline the implementation of cybersecurity policies. Moreover, incorporating IT expertise into HR-led initiatives ensures that training content remains relevant and up-to-date in the face of evolving threats.

Budget constraints are another significant barrier to implementing effective cybersecurity awareness programs, particularly in resource-limited settings. SMEs, in particular, face challenges in allocating sufficient resources for comprehensive training. This finding is consistent with previous research indicating that financial limitations often hinder the scalability and sustainability of cybersecurity initiatives (Cram et al., 2017). To address this issue, organizations could explore cost-effective alternatives, such as leveraging online platforms or partnering with external agencies to deliver training. Additionally, government

incentives or subsidies for cybersecurity training in SMEs could provide much-needed support for these organizations.

The dynamic nature of cyber threats further complicates the implementation of cybersecurity policies. The rapid evolution of attack vectors necessitates continuous updates to training programs to maintain their relevance. Gupta et al. (2019) emphasize the importance of adaptive training models that incorporate real-time threat intelligence and case studies of recent incidents. The findings suggest that organizations should adopt a proactive approach, regularly revisiting their training content to address emerging risks. Furthermore, incorporating predictive analytics into cybersecurity strategies could help organizations anticipate potential vulnerabilities and tailor their training accordingly.

The integration of metrics into cybersecurity awareness programs is another area warranting attention. While some organizations track employee participation in training sessions, fewer measure the actual impact of these programs on behavior and performance. Establishing clear metrics for evaluating the effectiveness of cybersecurity initiatives can provide valuable insights into areas for improvement. For example, metrics such as the reduction in successful phishing attempts or the frequency of password updates could serve as indicators of improved awareness. Ahmad et al. (2021) suggest that linking these metrics to organizational performance reviews could incentivize employees to actively participate in cybersecurity initiatives.

Another critical aspect is the role of hybrid work models in shaping cybersecurity awareness. The shift to remote work has blurred the boundaries between personal and professional digital spaces, introducing new risks. Furnell et al. (2020) highlight the challenges associated with securing personal devices used for work purposes, emphasizing the need for policies that address these vulnerabilities. The findings suggest that HR policies should include specific guidelines for remote work security, such as mandatory use of virtual private networks (VPNs) and regular updates to personal devices. Additionally, training programs should address the unique challenges of remote work, equipping employees with the skills to navigate these risks effectively.

Practical solutions for enhancing cybersecurity awareness must also consider the diversity of the workforce. The findings indicate that non-technical staff often exhibit lower levels of awareness, underscoring the need for role-specific training. Customizing content to address the specific responsibilities and risks associated with different roles can improve engagement and relevance. As noted by Shropshire et al. (2015), tailoring training to the needs of specific employee groups ensures that all members of the organization are adequately prepared to handle cyber threats.

The study's findings have broader implications for policy and practice. First, the integration of cybersecurity awareness into HR policies should be recognized as a strategic priority. Organizations must view cybersecurity not merely as a technical issue but as a fundamental aspect of operational resilience. This perspective requires a paradigm shift in how cybersecurity is approached, with greater emphasis on the human factors influencing security outcomes. Second, collaboration between academia, industry, and policymakers can drive the

development of innovative solutions to address the challenges identified in this study. For instance, partnerships between universities and organizations could facilitate the co-creation of training programs that leverage the latest research and technological advancements.

Finally, while this study provides valuable insights, it also highlights areas for future research. The findings suggest that further exploration is needed to understand the long-term impact of cybersecurity awareness programs on organizational resilience. Additionally, comparative studies across industries and geographies could provide a more comprehensive understanding of the contextual factors influencing the effectiveness of these initiatives. By addressing these gaps, future research can contribute to the development of more effective and inclusive cybersecurity policies.

Conclusion and Recommendation

This study highlights the pivotal role of HR policies in fostering cybersecurity awareness, emphasizing their integration into broader organizational strategies to address dynamic cyber threats. The findings reveal that tailored training programs, cross-departmental collaboration, and leadership support are critical for enhancing employee engagement and preparedness against cyber risks. However, challenges such as resource constraints, resistance to change, and rapidly evolving threats persist, underscoring the need for adaptive and scalable approaches. By linking cybersecurity awareness with organizational culture and leveraging innovative solutions like gamification and role-specific training, organizations can effectively mitigate vulnerabilities. The study contributes to the existing body of knowledge by offering insights into the interplay between HR policies and cybersecurity, while also identifying gaps in the alignment of training initiatives with emerging risks. These findings provide a foundation for future research to explore the long-term impacts of cybersecurity awareness programs, particularly in diverse organizational contexts, and to develop more comprehensive strategies for sustaining organizational resilience in an increasingly digitalized world.

References

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. Behaviour & Information Technology, 33(3), 237-248. https://doi.org/10.1080/0144929X.2012.708787

Ahmad, A., Maynard, S. B., & Park, S. (2021). Information security strategies: Towards an organizational multi-strategy perspective. Journal of Information Security and Applications, 59, 102805. https://doi.org/10.1016/j.jisa.2021.102805

Abrahams, Temitayo & Farayola, Oluwatoyin & Kaggwa, Simon & Uwaoma, Prisca & Hassan, Azeez & Dawodu, Samuel. (2024). CYBERSECURITY AWARENESS AND EDUCATION PROGRAMS: A REVIEW OF EMPLOYEE ENGAGEMENT AND ACCOUNTABILITY. Computer Science & IT Research Journal. 5. 100-119. 10.51594/csitrj.v5i1.708.

Alotaibi, M., & Almagwashi, H. (2021). Cybersecurity awareness in SMEs: Challenges and solutions. Journal of Information Security and Applications, 56, 102675. https://doi.org/10.1016/j.jisa.2021.102675

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. Computers & Security, 98, 102003. https://doi.org/10.1016/j.cose.2020.102003

Bada, Maria & Sasse, Angela & Nurse, Jason. (2015). Cyber Security Awareness Campaigns: Why do they fail to change behaviour?. 118-131..

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Choi, K., Levy, Y., & Hovav, A. (2018). The role of user computer self-efficacy, cybersecurity countermeasures awareness, and cybersecurity skills influence on computer misuse. Computers & Security, 87, 101583. https://doi.org/10.1016/j.cose.2018.06.018

Cram, W. A., D'Arcy, J., & Proudfoot, J. G. (2017). Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. MIS Quarterly, 41(1), 301-326.

Flick, U. (2018). An introduction to qualitative research. SAGE Publications.

Furnell, S., Clarke, N., & Lacey, D. (2020). Awareness, behavior, and culture: The ABC of cybersecurity culture. Computers & Security, 96, 101820. https://doi.org/10.1016/j.cose.2020.101820

Gupta, A., Dhillon, G., & Stahl, B. C. (2019). Information security policies and employee noncompliance: An empirical study. Information Systems Journal, 29(1), 43-58.

Hameed, A., & Khan, M. M. (2020). A cybersecurity awareness framework for managing human factors in the digital age. Journal of Information Security and Applications, 50, 102575. https://doi.org/10.1016/j.jisa.2020.102575

Harrison, B., Sanford, J., & Liu, L. (2021). Evaluating the impact of phishing simulation training on employee cybersecurity awareness. Journal of Information Technology Education, 20, 143-158.

Hillson, D., & Murray-Webster, R. (2017). Understanding and managing risk attitude. Routledge.

Koohang, A., Paliszkiewicz, J., & Goluchowski, J. (2021). Gamification in cybersecurity awareness: A review of effectiveness. Cybersecurity Journal, 4(3), 111–125.

Lincoln, Y. S., & Guba, E. G. (1985). Naturalistic inquiry. SAGE Publications.

Ng, B. Y., Kankanhalli, A., & Xu, Y. C. (2019). A theoretical model for cyber security risk analysis. MIS Quarterly, 33(4), 719-734.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security, 42, 165-176. https://doi.org/10.1016/j.cose.2013.12.003

Ponemon Institute. (2022). Cost of a Data Breach Report. IBM Security.

Tassabehji, R., Hackney, R., & Popovic, A. (2022). Strategic alignment of cybersecurity policies in organizations: A framework for success. Journal of Strategic Information Systems, 31(1), 101642. https://doi.org/10.1016/j.jsis.2022.101642

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

Yin, R. K. (2018). Case study research and applications: Design and methods (6th ed.). SAGE Publications.

Zhang, L., & McDowell, W. (2022). The effectiveness of cybersecurity training in mitigating cyber threats: An empirical analysis. Cybersecurity Research Journal, 9(2), 87-104.