Technology and Society Perspectives (TACIT) Vol. 2, No. 1, March 2024, pages 201–207

Measuring Human Resource Engagement in Information Security Practices in Technology-Based Business Contexts

Yudiyanto Joko Purnomo[1*]

[1]*Department of Management, Faculty of Economics, Universitas Nasional PASIM, Jawa Barat, Indonesia*

A R T I C L E I N F O

Article history:
Received: 18 March 2024
Revised: 21 March 2024
Accepted: 23 March 2024

DOI:
10.61100/tacit.v2i1.152

Keywords:
Human Resources, Information Security, Technology-Based Business

A B S T R A C T

Many businesses are currently transitioning to digital models, relying on information technology to store, manage, and process critical information. However, with increased technology usage, threats to information security are also on the rise. This research aims to measure the engagement of human resources in information security practices in the context of technology-based businesses. The research method employed is a qualitative literature review aimed at investigating various perspectives, approaches, and findings related to human resource engagement in information security practices in technology-based business contexts. Data for this literature review were obtained through searching scholarly articles using the Google Scholar search engine, spanning from 2006 to 2023. The study findings indicate that in the continuously evolving digital era, human resource engagement in information security practices is crucial for the success and sustainability of technology-based businesses. This responsibility extends beyond the IT department and involves collective responsibility throughout the organization. Measuring this engagement requires a holistic approach involving management, operational levels, and corporate culture.

A B S T R A K

Saat ini banyak bisnis yang beralih ke model digital, mengandalkan teknologi informasi untuk menyimpan, mengelola, dan memproses informasi penting. Namun, dengan peningkatan penggunaan teknologi, ancaman terhadap keamanan informasi juga semakin meningkat. Penelitian ini bertujuan untuk mengukur keterlibatan sumber daya manusia dalam praktik keamanan informasi di konteks bisnis berbasi teknologi. Metode penelitian ini merupakan sebuah tinjauan pustaka kualitatif yang bertujuan untuk menyelidiki berbagai pandangan, pendekatan, dan temuan terkait dengan keterlibatan sumber daya manusia dalam praktik keamanan informasi di konteks bisnis berbasis teknologi. Data untuk tinjauan pustaka ini diperoleh melalui pencarian artikel ilmiah menggunakan mesin pencari Google Scholar, dengan rentang waktu dari tahun 2020 hingga 2024. Hasil studi menunjukkan bahwa dalam era digital yang terus berkembang, keterlibatan sumber daya manusia dalam praktik keamanan informasi menjadi sangat penting bagi kesuksesan dan keberlangsungan bisnis berbasis teknologi. Hal ini bukan hanya tanggung jawab departemen IT, tetapi merupakan tanggung jawab bersama di seluruh organisasi. Mengukur keterlibatan ini memerlukan pendekatan holistik yang melibatkan manajemen, level operasional, dan budaya perusahaan.

1. INTRODUCTION

About 90% of the world's data has been created in the last two years. More businesses are shifting to digital models, relying on information technology to store, manage, and process crucial information (Verhoef et al., 2021). However, with the increased usage of technology, threats to information security are also escalating. Technology-based businesses have become prime targets for cyber-attacks, malware, and data breaches (Samara et al., 2023). Consequently, it is crucial for organizations to not only rely on technological solutions but also strengthen the human factor in their information security practices.

Human resources are valuable assets in ensuring effective information security (Rokhadi et al., 2023). Their engagement in information security practices is key to reducing organizational risks and vulnerabilities

** Corresponding author, email address: joko.jember2015@gmail.com*

to cyber threats. This involves understanding security policies, using appropriate security tools, and responding promptly to security threats. However, despite the importance of human resource engagement, a lack of security awareness, low compliance with security policies, and a shortage of technical skills in addressing cyber threats are common issues in many organizations.

Therefore, there is an urgent need to measure and enhance human resource engagement in information security practices. This involves not only proper training to increase awareness of security risks and compliance with policies but also the development of a strong security culture throughout the organization. A strong security culture will encourage employees to be proactive in protecting sensitive information and strengthen collaboration between information security departments and other departments within the organization (Van Niekerk & Von Solms, 2010).

Methods for measuring human resource engagement in information security practices need to be carefully developed. This should include objectively measurable indicators, such as the level of compliance with security policies, participation in security training, and response to security incidents. With appropriate methods, organizations can effectively monitor human resource engagement and identify areas where improvements are needed. Thus, research on measuring human resource engagement in information security practices in the context of technology-based businesses has significant implications. It will not only help improve the information security of organizations but also lay the groundwork for building a strong security culture that is the foundation for long-term success in this digital era.

2. THEORETICAL FRAMEWORK AND HYPOTHESES

Human Resources

Human resources refer to all the potential, skills, knowledge, and creativity of individuals involved in the operations and management of an organization (Susantinah et al., 2023). This encompasses all members of the organization, from entry-level employees to top-level managers, who contribute to the achievement of the company's goals and growth (Tusriyanto et al., 2023). Human resources also include aspects such as recruitment, training, development, performance management, and compensation, aimed at ensuring that the organization has a quality and skilled workforce to efficiently run its operations (Diawati et al., 2023; Prastyaningtyas et al., 2023). Additionally, human resources play a role in building a healthy organizational culture, creating an inclusive, productive, and motivating work environment for all team members (Kamar et al., 2022; Rustiawan et al., 2023). Thus, human resources are not only the most important asset to an organization but also a key factor in achieving competitive advantage and long-term success.

Information Security

Information security is the effort to protect sensitive and critical information from threats, risks, or vulnerabilities that may result in unauthorized or harmful access, disclosure, or use (Aslan et al., 2023). This includes protection of personal, financial, strategic, and other data, both in physical and digital forms. The goal of information security is to ensure that the information remains confidential, its integrity is preserved, and it is available only to authorized parties (Lundgren & Möller, 2019). To achieve this goal, organizations adopt various practices, policies, procedures, and technologies, such as data encryption, firewalls, access management, activity monitoring, security training, and risk management. Information security also involves aspects of organizational culture that promote security awareness, policy compliance, and collaboration among all members of the organization to mitigate threats and protect information effectively (Khando et al., 2021). With strong information security, organizations can reduce the risk of data loss, privacy breaches, financial losses, and reputational damage, as well as build trust with customers and business partners.

Technology-based Businesses

Technology-based businesses refer to businesses that heavily rely on the use of information and communication technology in various aspects of their operations (Qosasi et al., 2019). This includes the use of software, information systems, digital platforms, and other technology infrastructure to provide products or services, manage business processes, and interact with customers or business partners. Technology-based businesses often operate in industries such as information technology, e-commerce, fintech, telecommunications, software, and other digital services (Barbu et al., 2021). They leverage technological innovation to improve efficiency, increase productivity, create superior user experiences, and expand their market reach. Such businesses often serve as drivers of change in the economy, introducing new solutions, creating technology-based

jobs, and contributing to overall economic growth. Thus, technology-based businesses not only represent important trends in modern business development but also serve as centers of innovation and transformation in this digital era.

3. RESEARCH METHOD

The research method employed is a qualitative literature review aimed at investigating various perspectives, approaches, and findings related to human resource engagement in information security practices in the context of technology-based businesses. Data for this literature review were obtained through searching scholarly articles using the Google Scholar search engine, spanning from 2006 to 2023. In the initial search, a total of 50 articles were identified. However, to ensure accuracy, relevance, and quality, a rigorous selection involving evaluation of article titles, abstracts, and content was conducted. This selection was based on predefined inclusion criteria, including direct relevance to the research topic, research methods used, and relevance to the context of technology-based businesses. After going through this selection process, 25 final articles were chosen to be included in this literature review. Data from these articles will be qualitatively analyzed to identify patterns, themes, and emerging findings, as well as to gain a deep understanding of human resource engagement in information security practices in the context of technology-based businesses.

4. DATA ANALYSIS AND DISCUSSION

In the context of the ever-evolving digital era, information security practices play a crucial role as an indispensable component in efforts to maintain the success and operational continuity of technology-based businesses. Active involvement of human resources in implementing and maintaining information security levels is a crucial factor in preserving the integrity, confidentiality, and availability of data, which are valuable assets for companies.

The importance of human resource involvement in information security practices is undeniable. Human resources, as an integral aspect of organizational structure, serve as the primary pillar in ensuring the smooth operation of information security systems (Kukharska & Lagun, 2023). Especially in technology-dependent business contexts, where the need for information protection is increasingly pressing, the role of human resources in designing, implementing, and continuously improving information security practices becomes ever more vital. They are not only responsible for ensuring that technological infrastructure is equipped with effective security systems but also engaged in monitoring, evaluating, and developing security policies relevant to the ongoing technological changes. Therefore, proactively involving human resources in efforts to maintain information security is a necessity that cannot be overlooked in technology-oriented business strategies.

Initially, when evaluating the level of human resource involvement in information security practices, it is essential to emphasize that information security is not solely the responsibility of the IT department. This requires recognition that information security is a shared task that must be comprehensively implemented throughout the organizational structure. Thus, every individual involved, from managerial to operational levels, must have a profound understanding of the significance of information security and the impact of their contributions to its protection. This includes strengthening awareness of security practices, implementing appropriate policies, and readiness to participate in initiatives and developments aimed at enhancing overall information security levels. Therefore, positioning information security as a shared priority across all organizational layers will serve as a solid foundation for achieving success in maintaining the integrity and confidentiality of vital data for the operational continuity of the company (Willie, 2023).

At the managerial level, evaluating human resource involvement in information security practices can be done through the development of effective information security policies and the implementation of relevant procedures. Managers are responsible for ensuring that all team members have a deep understanding of these policies and can comply with every aspect of them (Kozlowski & Ilgen, 2006). This includes organizing periodic training sessions aimed at increasing awareness of information security and regularly monitoring compliance with established policies. Additionally, managers should be able to identify potential information security risks and take necessary preventive measures to reduce vulnerabilities. Human resource involvement in the managerial context not only involves policy implementation but also entails continuous efforts to improve awareness and ensure consistent compliance with established security standards.

At the operational level, human resource involvement is reflected in a strong awareness of threats to information security and actions necessary to maintain the integrity of company data. Education and training

related to information security are essential in this context (Sadiq Nasir, 2023). Employees need to be provided with a deep understanding of information security practices, including but not limited to, recognizing commonly used phishing techniques by attackers, implementing policies for secure password usage, and understanding the importance of promptly reporting security incidents. Furthermore, employees' roles in maintaining information security can be enhanced through the development of an organizational culture prioritizing security and providing appropriate incentives for compliance with security policies. Through heightened awareness and strong commitment at the operational level, companies can build a solid foundation in efforts to maintain the crucial information security vital for their operational continuity and business reputation.

Moreover, evaluating human resource involvement in information security practices can be seen through active contributions to the development and improvement of information security systems. Employees should feel encouraged to participate and invited to provide valuable input regarding initiatives to enhance overall information security levels. This may include involvement in security policy reviews and updates, identifying potential vulnerabilities, and implementing more effective preventive measures. Additionally, involving employees in decision-making related to information security not only strengthens their ownership of the process but also helps increase awareness and compliance with established policies. Reinforcing human resource involvement in the development and enhancement of information security aspects is key to maintaining the integrity and availability of data crucial for company operations (Kumah, 2022).

In the context of technology-dependent businesses, where companies are often targets of increasingly complex and serious cyberattacks, human resource involvement is not only a necessity but also an urgent requirement. Employees need to be seen as the first line of defense responsible for protecting valuable digital assets for the company. In response to these challenges, companies are obligated to implement sustainable investments in comprehensive training programs. This is intended to ensure that employees not only have a deep understanding of information security threats but also can quickly and effectively identify and respond to potential risks. Furthermore, companies must integrate human resource involvement in information security strategies as a top priority by encouraging active participation in the development and implementation of relevant security policies and procedures. Strengthening human resource involvement in efforts to protect company digital assets will be a crucial step in addressing increasingly sophisticated cyber threats (Saeed et al., 2023).

Measuring human resource involvement in information security practices in technology-driven businesses is not a simple task but a highly important and complex aspect. This process requires a comprehensive holistic approach involving all members of the organization from various levels, ranging from top management to the lowest operational level. Only by effectively implementing human resource involvement in every aspect of security policies and procedures can companies ensure that information security remains a top priority and their digital assets are optimally protected. This involves not only drafting appropriate policies but also providing continuous education and in-depth training for all personnel, as well as creating a corporate culture that fosters awareness and collective responsibility for information security. Integrating strong human resource involvement into information security strategies is key to maintaining the sustainability and reputation of the company in an era full of evolving security challenges.

Additionally, to measure human resource involvement in information security practices, there are additional steps that can be taken, one of which is evaluating the effectiveness of implemented training programs. Training programs should be carefully designed to strengthen employees' understanding of evolving information security threats and the latest techniques to combat such attacks (Alnajim et al., 2023). This evaluation can be conducted through various methods, such as knowledge tests to gauge understanding gained from training, participant satisfaction surveys to evaluate the effectiveness of the material taught, or even through increases in the quantity and quality of security incident reporting post-training. By considering the results of these evaluations, companies can make necessary adjustments to their training programs to ensure that employees have the knowledge and skills required to serve as a solid defense against information security threats.

Furthermore, the level of employee participation in information security initiatives can also be a crucial indicator of their involvement in security practices overall (Alkhazi et al., 2022). Evaluating this participation level can be done through various methods, including but not limited to, observing employees' compliance with established information security policies. This includes aspects such as using strong passwords, activating two-factor authentication, and complying with data access policies set by the company. Moreover,

employee participation in information security training programs, security-related group discussions, or even voluntary initiatives to report or respond to potential security threats can also be considered significant indicators of involvement. By considering these aspects, companies can gain a deeper understanding of the level of employee involvement in maintaining information security and identify areas where improvements or reinforcements are needed.

However, to achieve optimal levels of involvement in information security practices, it is important for organizations to build and promote a strong security culture. A mature security culture will ensure that information security is not merely seen as the responsibility of individuals or specific departments but rather ingrained in the overall identity and core values of the company (Da Veiga, 2016). To achieve this, organizations need to strengthen clear and consistent communication about the importance of information security at all levels, from management to operational-level employees. Additionally, recognition of good security practices should be highly regarded and openly acknowledged, thereby fostering a culture of awareness and responsibility for information security. Furthermore, recognizing human resources as crucial partners in the company's data protection efforts will strengthen the relationship between management and employees and foster effective collaboration in maintaining information security as a shared priority. In this way, organizations can build a solid foundation for effective information security practices, which are key to success and business continuity in the current digital era.

In addition to the aforementioned aspects, technology can also be used as a highly effective tool to measure human resource involvement in information security practices (Wahyoedi et al., 2023). For instance, the use of intuitive and user-friendly security incident reporting systems can greatly encourage employees to report incidents or suspicious events quickly and accurately, enabling security teams to respond promptly. Furthermore, the implementation of advanced analytical solutions to monitor compliance with information security policies can provide invaluable insights for organizations. By analyzing data comprehensively, analytical solutions can identify trends, patterns, and areas where improvements or enhancements in compliance are needed. By leveraging technology smartly and effectively, organizations can enhance transparency, accountability, and efficiency in their efforts to maintain vital information security.

Measuring human resource involvement in information security practices within technology-based businesses involves a complex and multidimensional approach, considering cultural, organizational, technological, and employee behavior factors. The importance of strengthening human resource involvement in information security practices cannot be overlooked, given the complexity and evolving vulnerabilities in today's digital environment. First and foremost, aspects of corporate culture, such as trust, norms, and values that promote awareness and responsibility towards information security, are key factors in determining the level of employee engagement. Furthermore, an organizational structure that supports and promotes teamwork, open communication, and transparency in information security policies also has a significant impact on human resource involvement. Additionally, the appropriate utilization of technology, such as integrated security incident reporting systems and advanced analytical solutions, can facilitate the measurement process and enhance the effectiveness of information security practices. Lastly, a deep understanding of employee behavior, including motivations, barriers, and preferences, is crucial in designing strategies to encourage sustained participation and involvement. Only through a holistic and integrated approach to all these dimensions can companies reduce information security risks and protect their digital assets more effectively amidst the evolving threats in today's digital world.

5. CONCLUSION, IMPLICATION, SUGGESTION, AND LIMITATIONS

In the continuously evolving digital era, the engagement of human resources in information security practices is paramount for the success and sustainability of technology-based businesses. This responsibility transcends beyond the IT department; it is a collective responsibility across the entire organization. Measuring this engagement requires a holistic approach involving management, operational levels, and corporate culture.

The importance of human resource engagement in information security practices underscores the need for investment in continuous training, development of effective policies, and fostering a strong security culture throughout the organization. It also signifies that success in maintaining information security depends not only on technology but also on the behavior and understanding of employees.

To enhance human resource engagement in information security practices, it is advisable for compa-

nies to adopt an inclusive and comprehensive approach. This entails developing clear policies, regular training, active participation in security system development, and cultivating a strong security culture. The use of technology can also facilitate the measurement and monitoring of employee engagement.

Although the importance of human resource engagement in information security practices is recognized, there are several limitations to consider. These include challenges in changing employee behavior, the cost and time required for implementing training programs, and the complexity of creating an effective security culture throughout the organization. Additionally, measuring this engagement can be challenging due to the subjective factors involved in assessment.

REFERENCES

Alkhazi, B., Alshaikh, M., Alkhezi, S., & Labbaci, H. (2022). Assessment of the Impact of Information Security Awareness Training Methods on Knowledge, Attitude, and Behavior. *IEEE Access*, *10*, 132132–132143. https://doi.org/10.1109/ACCESS.2022.3230286

Alnajim, A. M., Habib, S., Islam, M., AlRawashdeh, H. S., & Wasim, M. (2023). Exploring Cybersecurity Education and Training Techniques: A Comprehensive Review of Traditional, Virtual Reality, and Augmented Reality Approaches. *Symmetry*, *15*(12), 2175. https://doi.org/10.3390/sym15122175

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. *Electronics*, *12*(6), 1333. https://doi.org/10.3390/electronics12061333

Barbu, C. M., Florea, D. L., Dabija, D.-C., & Barbu, M. C. R. (2021). Customer Experience in Fintech. *Journal of Theoretical and Applied Electronic Commerce Research*, *16*(5), 1415–1433. https://doi.org/10.3390/jtaer16050080

Da Veiga, A. (2016). Comparing the information security culture of employees who had read the information security policy and those who had not. *Information & Computer Security*, *24*(2), 139–151. https://doi.org/10.1108/ICS-12-2015-0048

Diawati, P., Gadzali, S. S., Abd Aziz, M. K. N., Ausat, A. M. A., & Suherlan, S. (2023). The Role of Information Technology in Improving the Efficiency and Productivity of Human Resources in the Workplace. *Jurnal Teknologi Dan Sistem Informasi Bisnis*, *5*(3), 296–302. https://doi.org/https://doi.org/10.47233/jteksis.v5i3.872

Kamar, K., Lewaherilla, N. C., Ausat, A. M. A., Ukar, K., & Gadzali, S. S. (2022). The Influence of Information Technology and Human Resource Management Capabilities on SMEs Performance. *International Journal of Artificial Intelligence Research*, *6*(1.2), 1. https://doi.org/https://doi.org/10.29099/ijair.v6i1.2.676

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security*, *106*, 102267. https://doi.org/10.1016/j.cose.2021.102267

Kozlowski, S. W. J., & Ilgen, D. R. (2006). Enhancing the Effectiveness of Work Groups and Teams. *Psychological Science in the Public Interest*, *7*(3), 77–124. https://doi.org/10.1111/j.1529-1006.2006.00030.x

Kukharska, N., & Lagun, A. (2023). human resources management as a component of organization information security. *Cybersecurity: Education, Science, Technique*, *4*(20), 35–42. https://doi.org/10.28925/2663-4023.2023.20.3544

Kumah, P. (2022). The Role of Human Resource Management in Enhancing Organizational Information Systems Security. In *Research Anthology on Human Resource Practices for the Modern Workforce* (pp. 1251–1277). IGI Global. https://doi.org/10.4018/978-1-6684-3873-2.ch065

Lundgren, B., & Möller, N. (2019). Defining Information Security. *Science and Engineering Ethics*, *25*(2), 419–441. https://doi.org/10.1007/s11948-017-9992-1

Prastyaningtyas, E. W., Ausat, A. M. A., Muhamad, L. F., Wanof, M. I., & Suherlan, S. (2023). The Role of Information Technology in Improving Human Resources Career Development. *Jurnal Teknologi Dan Sistem Informasi Bisnis*, *5*(3), 266–275. https://doi.org/https://doi.org/10.47233/jteksis.v5i3.870

Qosasi, A., Maulina, E., Purnomo, M., Muftiadi, A., Permana, E., & Febrian, F. (2019). The Impact of Information and Communication Technology Capability on the Competitive Advantage of Small Businesses. *International Journal of Technology*, *10*(1), 167. https://doi.org/10.14716/ijtech.v10i1.2332

Rokhadi, R., Sukistanto, S., Hariyanti, H., & Mariyani, D. (2023). Management Strategies to Address Human Resources Challenges in the Information Technology Era. *Jurnal Minfo Polgan*, *12*(2), 2082–2090. https://doi.org/10.33395/jmp.v12i2.13152

Rustiawan, I., Gadzali, S. S., Suharyat, Y., Iswadi, U., & Ausat, A. M. A. (2023). The Strategic Role of Human Resource Management in Achieving Organisational Goals. *Innovative: Journal Of Social Science Research*, *3*(2), 632–642. https://doi.org/https://doi.org/10.31004/innovative.v3i2.345

Sadiq Nasir. (2023). Exploring the Effectiveness of Cybersecurity Training Programs: Factors, Best Practices, and Future Directions. *Advances in Multidisciplinary and Scientific Research Journal Publication*, *2*(1), 151–160. https://doi.org/10.22624/AIMS/CSEAN-SMART2023P18

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. *Sensors*, *23*(15), 6666. https://doi.org/10.3390/s23156666

Samara, E., Andronikidis, A., Komninos, N., Bakouros, Y., & Katsoras, E. (2023). The Role of Digital Technologies for Regional Development: a System Dynamics Analysis. *Journal of the Knowledge Economy*, *14*(3), 2215–2237. https://doi.org/10.1007/s13132-022-00951-w

Susantinah, N., Krishernawan, I., & Murthada. (2023). Human Resource Management (HRM) Strategy in Improving Organisational Innovation. *Journal of Contemporary Administration and Management (ADMAN)*, *1*(3), 201–207. https://doi.org/10.61100/adman.v1i3.80

Tusriyanto, Sulaeman, Moh. M., & Nurcholidah, L. (2023). Optimising Organisational Performance Through Human Resource Management Strategy and Technology Integration to Enhance Innovation. *Technology and Society Perspectives (TACIT)*, *1*(3), 139–147. https://doi.org/https://doi.org/10.61100/tacit.v1i3.81

Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security*, *29*(4), 476–486. https://doi.org/10.1016/j.cose.2009.10.005

Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Qi Dong, J., Fabian, N., & Haenlein, M. (2021). Digital transformation: A multidisciplinary reflection and research agenda. *Journal of Business Research*, *122*, 889–901. https://doi.org/10.1016/j.jbusres.2019.09.022

Wahyoedi, S., Suherlan, S., Rijal, S., Azzaakiyyah, H. K., & Ausat, A. M. A. (2023). Implementation of Information Technology in Human Resource Management. *Al-Buhuts*, *19*(1), 300–318. https://doi.org/https://doi.org/10.30603/ab.v19i1.3407

Willie, M. M. (2023). The Role of Organizational Culture in Cybersecurity: Building a Security-First Culture. *Journal of Research, Innovation and Technologies (JoRIT)*, *2*(16), 180. https://doi.org/10.57017/jorit.v2.2(4).05