Technology and Society Perspectives (TACIT) Vol. 2, No. 1, March 2024, pages 165–192

Organizational and Social Factor Analysis: The Role of Human Resources in the Success of Information Security Systems in the Digital Business Context

Budi Sunarso[1*]

[1]*Universitas Islam Negeri (UIN) Salatiga, Jawa Tengah, Indonesia*

A R T I C L E I N F O

Article history:
Received: 9 March 2024
Revised: 13 March 2024
Accepted: 15 March 2024

DOI:
10.61100/tacit.v2i1.143

Keywords:
Organization, Social, Human Resources, Information Security Systems, Digital Business

A B S T R A C T

In the continually evolving digital business era, information security has become paramount for organizations to ensure the continuity of their operations. Information security systems involve not only technology but also organizational and social factors that play a crucial role in managing human resources. This research aims to conduct an in-depth analysis of how human resources can influence the success of information security systems in the context of digital business. The research method employed in this study is a qualitative literature review with data collection from Google Scholar for the years 2006-2024. The study findings indicate that in the ever-evolving digital era, information security is crucial in the context of digital business. Information security systems rely not only on technology but also on organizational, social, and human factors. Effective integration of technology, organization, and human resources is key to creating a strong and adaptive information security environment.

A B S T R A K

Dalam era bisnis digital yang terus berkembang, keamanan informasi telah menjadi hal yang sangat penting bagi organisasi untuk memastikan keberlangsungan operasi mereka. Sistem keamanan informasi tidak hanya melibatkan teknologi, tetapi juga faktor organisasi dan sosial yang berperan dalam mengelola sumber daya manusia. Penelitian ini bertujuan untuk melakukan analisis mendalam tentang bagaimana sumber daya manusia dapat memengaruhi keberhasilan sistem keamanan informasi dalam konteks bisnis digital. Metode penelitian yang digunakan dalam penelitian ini adalah tinjauan pustaka kualitatif dengan pengambilan data dari Google Scholar tahun 2006-2024. Hasil studi menunjukkan bahwa dalam era digital yang terus berkembang, keamanan informasi menjadi krusial dalam konteks bisnis digital. Sistem keamanan informasi tidak hanya bergantung pada teknologi, tetapi juga pada faktor organisasi, sosial, dan manusia. Integrasi yang efektif antara teknologi, organisasi, dan sumber daya manusia menjadi kunci utama dalam menciptakan lingkungan keamanan informasi yang kuat dan adaptif.

1. INTRODUCTION

In the ever-evolving digital business era, information security has become critical for organisations to ensure the continuity of their operations (Safitra et al., 2023). Information security systems involve not only technology, but also organisational and social factors that play a role in managing human resources. The success of information security systems in the context of digital business depends heavily on these factors.

Significant changes in the business paradigm of organisations are occurring along with the emergence of the digital transformation phenomenon. Businesses that adopt the digital model proactively utilise information and communication technologies to streamline their operational processes, expand market reach, and increase productivity (Arjang et al., 2023). Nonetheless, with the increasing integration of technology in business operations, attention to information security has become increasingly urgent. This phenomenon marks a challenge that must be effectively addressed by organisations that want to harness the full potential of digital transformation without compromising the security of vital data and information.

Information is considered a highly valuable asset for any organisational entity, given that any loss

** Corresponding author, email address: sunarsobudi77@gmail.com*

or unintended disclosure of such information has the potential to seriously impact a company's public image, financial stability, and operational continuity (Juma'h & Alnsour, 2020). Threats to information security can arise from a variety of sources, which include hacking attacks, malware infections, data leakage incidents, and insider threats originating from individuals who have access to the organisation's internal systems.

Various internal aspects including security policies, organisational culture, hierarchical structure, and internal communication within an organisational entity play an important role in determining the success of an information security system (da Veiga et al., 2020). Past research has revealed that the level of management awareness and commitment to information security, along with the active participation of employees in the implementation of security policies, has a significant impact on the overall effectiveness of the information security system (Khando et al., 2021). These internal factors interact with each other in a complex manner and contribute to the formation of a supportive work environment in protecting the organisation's information assets from various threats and risks that may arise.

Social factors, which include individual user behaviour and interaction dynamics within the organisational context, also play an important role in influencing the level of information security (Simonet & Teufel, 2019). For example, the level of employee awareness of and compliance with security policies, along with the level of collaboration and communication between departments, can have significant implications for the information security risks faced by an organisation. Individual awareness of digital security practices and vigilance against potential cyber threats, together with strong cooperation and effective communication flows between organisational units, form a strong foundation in mitigating risks related to the organisation's overall information security.

Human resources play a central role in determining the success of an organisation's information security system. Information security-focused employee training and development initiatives, security-appropriate personnel recruitment and selection strategies, and the implementation of effective performance management practices all have a significant impact on maintaining the integrity and confidentiality of an organisation's information (Fianty, 2023). This holistic approach to people management not only strengthens individuals' ability to address digital security threats, but also creates a security-oriented organisational culture, where awareness of the importance of protecting sensitive information becomes an integral part of every aspect of operations.

Taking into account the complexity of digital business, as well as the important role of organisational and social factors in the success of information security systems, this research aims to conduct an in-depth analysis of how human resources can influence the success of information security systems in the context of digital business. With a better understanding of the factors that influence information security, organisations can develop more effective strategies to protect their information assets and reduce security risks.

2. THEORETICAL FRAMEWORK AND HYPOTHESES

Organization

An organization is a structured and organized entity, akin to a complex network comprising individuals, departments, and processes interconnected to achieve common goals (Barker Scott & Manning, 2024). Like a growing tree, organizations have roots underlying their structure and culture, a trunk supporting policies and procedures, and branches representing various departments and functions. Like a winding river, interactions and communications among organizational members flow and branch out, forming complex and dynamic networks of relationships. As a living entity, organizations continually adapt to their external environment, responding to market changes, regulations, and technology (Ausat & Suherlan, 2021). Like an orchestra composed of various instruments, organizations require coordination and harmony among different elements to achieve optimal performance and realize their vision and mission. Thus, an organization is a system consisting of many interconnected components that interact to achieve common goals.

Social

Social refers to the interactions, relationships, and dynamics among individuals within a community or society (Anna Yohanna, 2020). Like interconnected neural networks, the social dimension creates complex patterns in human life, encompassing norms, values, and communication processes that shape collective identity and behavioral patterns. Like binding ties, social interactions form relationships among individuals based on similarities, differences, or shared goals, creating social networks that connect people in various contexts, from family and friends to communities and organizations (Litt et al., 2020). Like a fertile garden, the social

environment provides a space for growth, learning, and adaptation, enabling individuals to understand and respond to changes in values, culture, and technology. Like a mirror reflecting, social interactions create self-reflection and identity recognition, enriching individuals' life experiences through understanding, empathy, and solidarity with others (Segal, 2011). Thus, the social dimension not only describes human interconnectedness but also provides the foundation for constructing and maintaining networks of relationships that enrich and strengthen human life collectively.

Human Resources (HR)
Human Resources (HR) refers to essential elements within an organization comprising individuals working within it, directly or indirectly, to achieve organizational goals (Rustiawan et al., 2023). Like wheels driving a machine, HR is a dynamic force that propels organizational activities and productivity, encompassing skills, knowledge, experience, and personal qualities of each individual (Susantinah et al., 2023). Like a core shaping the center of strength, HR influences organizational performance and effectiveness through recruitment, training, development, and efficient performance management (Tusriyanto et al., 2023). Like seeds planted in fertile soil, investment in HR has the potential to yield abundant results in the form of innovation, creativity, and adaptation to environmental changes. Like neural networks regulating bodily functions, HR creates complex and interconnected relationships among individuals in the organization, facilitating collaboration, communication, and knowledge exchange (Diawati et al., 2023). Thus, HR is not only a critical organizational component but also a vital force shaping and driving internal organizational dynamics, influencing its overall performance and success.

Information Security System (ISS)
Information Security System (ISS) refers to a set of strategies, policies, and technologies designed to protect sensitive and critical information from threats, misuse, or unauthorized access (Ahmad et al., 2014). Like fences protecting a house from intrusion, ISS aims to establish strong defense layers to safeguard the integrity, confidentiality, and availability of information within an organization or system. Like keys securing a door, ISS involves the use of encryption, authentication, and authorization technologies to ensure that only authorized users can access sensitive information (Koo et al., 2020). Like vigilant fire systems, ISS also involves threat monitoring and detection, as well as rapid response to security incidents to minimize their negative impacts. Like a sturdy foundation, ISS requires careful planning and implementation, as well as continuous maintenance to keep it relevant in the face of evolving security threats (Tariq et al., 2023). Thus, ISS is not just a collection of tools and techniques but also a holistic approach that considers technical, policy, and human aspects in protecting valuable information assets.

Digital Business
Digital business is a form of economic activity that relies on information and communication technology (ICT) as its primary foundation to conduct operations, interact with customers, and carry out business transactions online (Harahap et al., 2023). Like an unlimited global network, digital business leverages the internet and other digital platforms to connect customers with products and services, unrestricted by geographical or time boundaries (Sudirjo et al., 2023). Like a constantly changing landscape, digital businesses continuously adapt to new technological developments and market trends, creating new opportunities and ongoing challenges. Like a machine that never stops, digital businesses operate in a dynamic and rapidly changing environment, allowing high flexibility and scalability in responding to diverse market demands. Like interconnected ecosystems, digital businesses also enable collaboration among companies, partners, and consumers across various platforms and channels, creating greater value for all stakeholders (Agustian et al., 2023). Thus, digital business is not just a transformation from traditional business models to the online realm but also a new paradigm in how organizations interact, innovate, and grow in the continually evolving digital era.

3. RESEARCH METHOD
The research method used in this study is a qualitative literature review with data collection from Google Scholar for the years 2006-2024. A qualitative approach is used to deeply understand concepts and theories related to organizational and social factors in the success of information security systems in the context of digital business. By analyzing various articles, journals, and scholarly publications available on Google

Scholar during the period from 2006 to 2024, this research aims to provide a comprehensive overview of existing understanding, current trends, and research contributions in this field. Through qualitative literature review, this study will identify and analyze various approaches, theories, methodologies, and relevant findings put forward by previous researchers, as well as formulate a conceptual framework that will serve as the basis for further research in this area.

4. DATA ANALYSIS AND DISCUSSION

In the ever-evolving digital era, information security is one of the critical aspects that cannot be ignored in the context of digital business. Given the rapid growth rate of information technology and the increasing complexity of security threats, information security systems are the main foundation in maintaining the integrity, confidentiality and availability of data and services vital to digital business operations. However, the success of information security systems is not solely determined by technology. Organisational and social factors also play a significant role in determining the effectiveness of information security systems in the context of digital business (Solomon & Brown, 2021).

Analysis of organisational factors in the context of the success of information security systems includes various aspects that play a crucial role. One of them is the existence of a clearly defined and well-organised organisational structure, which is a prerequisite for assigning appropriate responsibilities related to information security (Blum, 2020). In addition, the involvement and strong support of the highest levels of leadership in the organisation is crucial, whether in setting relevant security policies, allocating adequate resources or promoting an organisational culture that encourages security awareness (Zen et al., 2023). In this context, the role of top leadership is not only limited to setting strategic direction, but also building a cultural foundation that prioritises information security as an integral part of every aspect of operations and decision-making. The synergistic integration of a solid organisational structure and high commitment from organisational leaders is an important element in building and maintaining an effective and adaptive information security system in the face of evolving challenges in the digital era.

In addition to the factors already mentioned, organisational culture plays a significant role in determining the success of information security systems. A culture that promotes information security awareness, transparency and mutual trust among organisational members has a positive impact on reducing the risk of security incidents that may arise due to human error or insecure behaviour (Thomson et al., 2006). Developing regular information security training and awareness initiatives is also critical in improving employees' understanding and skills in facing and addressing evolving and complex security threats. A strong organisational culture in information security not only creates a safe and secure environment for its members but also positively impacts the integrity of the information security system as a whole, making it a key aspect in the overall strategy to protect business assets and operations in the dynamic digital age.

Besides organisational factors, social factors also have significant implications for the success of information security systems in the context of digital business. The dynamics of interaction between individuals inside and outside the organisation play an important role in information security arrangements. Collaboration between departments or business units within the organisation, as well as cooperation with business partners and other external entities, requires building trust and mutual understanding of needs and responsibilities in the context of information security (Castañer & Oliveira, 2020). This process involves not only the effective exchange of information, but also a concerted effort to reinforce security principles at every stage of co-operation. By paying attention to this social dimension, organisations can optimise collaboration and minimise security risks that may arise from a lack of understanding or trust among stakeholders. Thus, understanding and handling social factors wisely is key to building a robust and sustainable information security system in the evolving digital business environment.

In the context of information security management, human factors or human resources play a central role in all aspects, from management to implementation of policies and procedures related to information security. The success of an information security system relies heavily on employees who are well trained, have adequate technical skills, and above all have a deep awareness of the importance of maintaining information security (He & Zhang, 2019). They become valuable assets to the organisation in protecting information assets from increasingly diverse and complex cyber threats. In addition, the active involvement of employees in keeping abreast of technological developments and information security trends also plays a role in strengthening an organisation's defences against cyber-attacks. Investing in employee development, both through regular training and efforts to raise information security awareness, is a crucial step in building

a strong security culture that is responsive to evolving information security challenges.

In navigating the complexities of digital business, the success of information security systems does not depend solely on technological advances, but also depends on the harmonious interaction and integration of organisational, social and human resource factors. Apart from advanced technological capabilities, factors such as a well-defined organisational structure, an internalised security culture, and the active involvement and high awareness of employees are key in building and maintaining a robust information security environment. The collaboration of advanced technology with a responsive organisational structure and a security-first organisational culture will create a solid foundation in the face of ever-evolving challenges in a dynamic digital world. In this context, the importance of effective integration between technology, organisation and people cannot be overstated, as this becomes the main foundation in delivering an information security environment that is adaptive and responsive to the ongoing dynamics of change.

Effective integration of technology, organisation and people is not only the key, but also the essential foundation in creating a robust and adaptive information security environment in the face of complex challenges in the dynamic digital era. A holistic strategy that embraces these dimensions is imperative in upholding information security in the evolving digital business context. This involves the implementation of advanced security technologies to identify and protect sensitive data, the development of an organisational culture that emphasises the importance of security as a top priority, and continued investment in human resource development and training (Cremer et al., 2022). Thus, while technology provides a strong foundation, organisational and human factors provide a human dimension that cannot be overlooked in the effort to strengthen and sustain an effective information security system amidst the relentless flow of change in the digital world.

Nonetheless, the challenges organisations face in managing human resources to achieve optimal information security are numerous. There is an urgent need to continuously upgrade the skills, both technical and non-technical, of employees to be able to effectively address and respond to evolving and increasingly complex security threats. In addition, organisations are also faced with the challenging task of attracting, retaining and developing the best talent in the information security field (Junça Silva & Dias, 2023). This is becoming increasingly important given the high demand and fierce competition for qualified labour in the ever-evolving information security industry. In this context, a comprehensive strategy in human resource management is crucial, not only to meet current needs but also to prepare organisations for the unforeseen challenges and opportunities of the future.

In the face of these complex challenges, organisations can take a proactive approach to human capital management to strengthen information security. This approach includes a variety of strategies that reflect the organisation's commitment to dealing effectively with security threats. One key strategy is through investment in training and certification programmes designed to enhance employees' technical skills in the face of increasingly complex and dynamic security threats (Morandini et al., 2023). In addition, organisations can also design attractive incentive and promotion programs for information security professionals, which can help attract and retain the best talent in the industry. At a deeper level, building an organisational culture that places information security as a top priority is essential. This involves establishing norms and values that promote security awareness and placing a strong emphasis on security practices in every aspect of the organisation's operations. By adopting this approach, organisations can strengthen their ability to protect information assets and respond effectively to evolving security threats.

In addition to the internal strategies discussed earlier, collaboration between organisations and educational institutions can also be a valuable asset in the effort to improve capability and capacity in managing information security. Well-designed internship programmes, research collaborations and knowledge exchanges between industry and educational institutions are concrete steps that can strengthen the information security human resource development ecosystem. Through such programmes, organisations can gain access to passionate and innovative young talent, while educational institutions can gain first-hand insights into industry demands and the latest trends and challenges in information security. Such collaborations not only have the potential to enhance the skills and knowledge of students and interns, but also enable more efficient adoption of industry best practices. By building a strong partnership between the education and industry sectors, a sustainable ecosystem can be created, which in turn will support the development of qualified and competitive human resources in the information security field.

With an awareness of the important role played by human resources in achieving a successful infor-

mation security system, organisations can build a solid foundation to face the increasingly complex and diverse challenges in the digital business domain. Thus, it is undeniable that effective integration between organisational, social and human factors is the key to achieving success in managing information security in the ever-evolving digital era. In this context, human resource management is not only seen as a purely administrative task, but also as a critical strategy in building organisational capacity to respond quickly and effectively to changes occurring in a dynamic business environment. Therefore, investment in skills development, promotion of a strong security culture, and collaboration with educational institutions and industry partners are important steps in optimising the potential of human resources to support the organisation's overall information security. With a comprehensive and integrated approach, organisations can strengthen their resilience to evolving security threats, making it an integral part of the overall strategy to achieve excellence in a dynamic digital business world.

5. CONCLUSION, IMPLICATION, SUGGESTION, AND LIMITATIONS

In the ever-evolving digital era, information security is crucial in the context of digital business. Information security systems depend not only on technology, but also on organisational, social and human factors. Effective integration of technology, organisation and human resources is key to creating a robust and adaptive information security environment. The importance of considering organisational, social and human aspects in information security management has major implications for digital business planning and strategy. Organisational leadership must be actively involved in setting security policies, allocating resources and promoting a strong security culture. Regular information security training and awareness is also important to reduce the risk of security incidents.

Organisations need to adopt a proactive approach to human resource management for information security. Investments in training programmes, certifications, and attractive incentives and promotions for information security professionals can help attract, retain and develop top talent. Collaboration between industry and educational institutions is also important in improving capability and capacity in managing information security. While integration between technology, organisation and people is important, managing human resources for information security is not easy. Challenges include developing employees' technical and non-technical skills, as well as fierce competition for qualified labour. In addition, collaborative efforts also require significant time and commitment from all parties involved.

REFERENCES

Agustian, K., Mubarok, E. S., Zen, A., Wiwin, W., & Malik, A. J. (2023). The Impact of Digital Transformation on Business Models and Competitive Advantage. *Technology and Society Perspectives (TACIT)*, *1*(2), 79–93. https://doi.org/10.61100/tacit.v1i2.55

Ahmad, A., Maynard, S. B., & Park, S. (2014). Information security strategies: towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing*, *25*(2), 357–370. https://doi.org/10.1007/s10845-012-0683-0

Anna Yohanna. (2020). The influence of social media on social interactions among students. *Indonesian Journal of Social Sciences*, *12*(2), 34–48.

Arjang, A., Sutrisno, S., Permana, R. M., Kusumastuti, R., & Ausat, A. M. A. (2023). Strategies for Improving the Competitiveness of MSMEs through the Utilisation of Information and Communication Technology. *Al-Buhuts*, *19*(1), 462–478.

Ausat, A. M. A., & Suherlan, S. (2021). Obstacles and Solutions of MSMEs in Electronic Commerce during Covid-19 Pandemic: Evidence from Indonesia. *BASKARA: Journal of Business and Entrepreneurship*, *4*(1), 11–19. https://doi.org/10.54268/BASKARA.4.1.11-19

Barker Scott, B. A., & Manning, M. R. (2024). Designing the Collaborative Organization: A Framework for how Collaborative Work, Relationships, and Behaviors Generate Collaborative Capacity. *The Journal of Applied Behavioral Science*, *60*(1), 149–193. https://doi.org/10.1177/00218863221106245

Blum, D. (2020). Put the Right Security Governance Model in Place. In *Rational Cybersecurity for Business* (pp. 61–89). Apress. https://doi.org/10.1007/978-1-4842-5952-8_3

Castañer, X., & Oliveira, N. (2020). Collaboration, Coordination, and Cooperation Among Organizations: Establishing the Distinctive Meanings of These Terms Through a Systematic Literature Review. *Journal of Management*, *46*(6), 965–1001. https://doi.org/10.1177/0149206320901565

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk

and cybersecurity: a systematic review of data availability. *The Geneva Papers on Risk and Insurance - Issues and Practice*, *47*(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6

da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security*, *92*, 101713. https://doi.org/10.1016/j.cose.2020.101713

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

Fianty, M. I. (2023). The Impact of Employees' Information Security Awareness on Information Security Behaviour. *International Journal of Information System & Technology*, *6*(5), 629–636.

Harahap, M. A. K., Sutrisno, S., Fauzi, F., Jusman, I. A., & Ausat, A. M. A. (2023). The Impact of Digital Technology on Employee Job Stress: A Business Psychology Review. *Jurnal Pendidikan Tambusai*, *7*(1), 3635–3638. https://jptam.org/index.php/jptam/article/view/5775

He, W., & Zhang, Z. (Justin). (2019). Enterprise cybersecurity training and awareness programs: Recommendations for success. *Journal of Organizational Computing and Electronic Commerce*, *29*(4), 249–257. https://doi.org/10.1080/10919392.2019.1611528

Juma'h, A. H., & Alnsour, Y. (2020). The effect of data breaches on company performance. *International Journal of Accounting & Information Management*, *28*(2), 275–301. https://doi.org/10.1108/IJAIM-01-2019-0006

Junça Silva, A., & Dias, H. (2023). The relationship between employer branding, corporate reputation and intention to apply to a job offer. *International Journal of Organizational Analysis*, *31*(8), 1–16. https://doi.org/10.1108/IJOA-01-2022-3129

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

Koo, J., Kang, G., & Kim, Y.-G. (2020). Security and Privacy in Big Data Life Cycle: A Survey and Open Challenges. *Sustainability*, *12*(24), 10571. https://doi.org/10.3390/su122410571

Litt, E., Zhao, S., Kraut, R., & Burke, M. (2020). What Are Meaningful Social Interactions in Today's Media Landscape? A Cross-Cultural Survey. *Social Media + Society*, *6*(3), 1–17. https://doi.org/10.1177/2056305120942888

Morandini, S., Fraboni, F., De Angelis, M., Puzzo, G., Giusino, D., & Pietrantoni, L. (2023). The Impact of Artificial Intelligence on Workers' Skills: Upskilling and Reskilling in Organisations. *Informing Science: The International Journal of an Emerging Transdiscipline*, *26*, 039–068. https://doi.org/10.28945/5078

Rustiawan, I., Amory, J. D. S., & Kristanti, D. (2023). The Importance of Creativity in Human Resource Management to Achieve Effective Administration. *Journal of Contemporary Administration and Management (ADMAN)*, *1*(3), 144–149. https://doi.org/10.61100/adman.v1i3.63

Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. *Sustainability*, *15*(18), 13369. https://doi.org/10.3390/su151813369

Segal, E. A. (2011). Social Empathy: A Model Built on Empathy, Contextual Understanding, and Social Responsibility That Promotes Social Justice. *Journal of Social Service Research*, *37*(3), 266–277. https://doi.org/10.1080/01488376.2011.564040

Simonet, J., & Teufel, S. (2019). The Influence of Organizational, Social and Personal Factors on Cybersecurity Awareness and Behavior of Home Computer Users. In *ICT Systems Security and Privacy Protection* (pp. 194–208). https://doi.org/10.1007/978-3-030-22312-0_14

Solomon, G., & Brown, I. (2021). The influence of organisational culture and information security culture on employee compliance behaviour. *Journal of Enterprise Information Management*, *34*(4), 1203–1228. https://doi.org/10.1108/JEIM-08-2019-0217

Sudirjo, F., Ausat, A. M. A., Rijal, S., Riady, Y., & Suherlan, S. (2023). ChatGPT: Improving Communication Efficiency and Business Management of MSMEs in the Digital Age. *Innovative: Journal Of Social Science Research*, *3*(2), 643–652. https://doi.org/https://doi.org/10.31004/innovative.v3i2.347

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

Tariq, U., Ahmed, I., Bashir, A. K., & Shaukat, K. (2023). A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review. *Sensors*, *23*(8), 4117. https://doi.org/10.3390/s23084117

Thomson, K.-L., von Solms, R., & Louw, L. (2006). Cultivating an organizational information security culture. *Computer Fraud & Security*, *2006*(10), 7–11. https://doi.org/10.1016/S1361-3723(06)70430-4

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

Zen, A., Yanti, S., Hutomo, M. R., Kraugusteeliana, K., & Arisutama, H. Y. (2023). The Role of Leadership in Managing Organisational Culture Change in the Context of Information Technology Implementation. *Jurnal Minfo Polgan*, *12*(1), 1247–1255. https://doi.org/10.33395/jmp.v12i1.12697