Proceedings of the 10th World Congress on Electrical Engineering and Computer Systems and Sciences (EECSS'24)
Barcelona, Spain - August 19 - 21, 2024
Paper No. CIST 163
DOI: 10.11159/cist24.163

Enhancing Organizational Success through Knowledge Sharing and Information Security Governance: A Comprehensive Survey

Razan AITooq[1], Nada Barnawi[2], Dr.Ahmad Alhamed[3]
Information Systems Department / King Saud University
Riyadh 11362, Saudi Arabia
First. raltoq@ksu.edu.sa; Second.nbarnawi@ksu.edu.sa; Third. aalhamed@ksu.edu.sa

Abstract **-** In today's organizational landscape, knowledge sharing and information security have evolved into fundamental concepts. They serve to bolster organizational responsibility and practices aimed at achieving various goals, including objective attainment and risk management. Knowledge sharing, when seamlessly integrated with a robust security framework, emerges as a critical driver of organizational success. Consequently, organizations consistently strive to leverage existing knowledge to enhance their objectives, exploring novel avenues to augment knowledge-sharing activities and foster a culture of knowledge exchange among employees, partners, and suppliers. This research endeavors to delineate the benefits of knowledge sharing and its role in fortifying organizational strategy and procedures, thereby mitigating risk. It identifies factors influencing knowledge sharing among employees and elucidates potential barriers that impede such sharing.

Keywords**:** Knowledge Sharing, Information Security, Governance, Organizational Strategy, and Risk Management

1. Introduction

Management plays a crucial role in information security governance, significantly impacting organizational behaviors. Effective management of information security requires the development and implementation of comprehensive policies that encompass awareness of organizational assets, compliance training, establishment of a robust institutional information structure, and alignment of business, IT, and human resource management [1]. In today's knowledge-dependent landscape, organizational success hinges on effective knowledge management. Sharing knowledge in accordance with well-defined policies can foster organizational growth and prosperity, underscoring the pivotal role of knowledge in organizational success.

The imperative for organizations to prioritize information security at the governance level is evident, with knowledge sharing emerging as a cornerstone concept and information security management a critical facet of organizational governance. Within organizations, governance encompasses various tasks, including supporting senior management in understanding and disseminating information policies, training employees on compliance with information protection protocols, delineating permissible information sharing practices, and integrating technical and administrative activities to ensure policy success [1].

Information management frameworks such as COBIT or ISO27001 can bolster information security by developing governance approaches that mitigate risks, enabling the formulation of security policies and procedures conducive to knowledge exchange [2]. Compliance with organizational information security policies and procedures is paramount, with adherence to policies, active participation in information security initiatives, and personal conviction in the importance of safeguarding information assets serving as key drivers. Notably, hiring employees who align with organizational information security policies significantly enhances policy adherence [3].

Attitude plays a pivotal role in shaping behavior, with positive attitudes towards organizational information security policies correlating with higher levels of compliance [3]. Reinforcing positive attitudes towards these policies can thus foster a culture of compliance within organizations.

The subsequent sections delve into a comprehensive literature review, elucidating factors influencing knowledge sharing, its benefits, and potential barriers.

2. Literature Review

This section presents the research proposals related to knowledge sharing and information security in organizations, which were published in recent years.

Skopik et al. [4] provide a structured overview of cyber security information sharing dimensions. They articulate the need for enhanced information-sharing systems and outline legal considerations and standardization efforts. Moreover, they highlight critical factors for building future security information-sharing platforms.

Jen et al. [5] conducted an empirical survey in southeastern China, revealing that risk-sharing and trust contracting increase knowledge sharing among supply chain partners, thereby enhancing overall supply chain performance. Their research emphasizes the importance of corporate governance mechanisms for knowledge and supply chain management, along with best practices for knowledge sharing in supply chains.

Goffnett and Williams [6] emphasize that trust fosters stronger collaborative partnerships among alliance members, leading to efficient knowledge sharing. Similarly, Charterina et al. [7] assert that sharing knowledge enhances alliance partners' performance by facilitating timely logistics decisions and reducing total costs.

Safa et al. [8] investigate information security collaboration (ISC) within organizations, finding that personal norms, involvement, and commitment significantly influence employees' attitude towards ISC intention.

Xuan [9] proposes recommendations to enhance knowledge-sharing motivation among Vietnamese SME employees. The author identifies factors such as teamwork, cohesion, trust, reward systems, and senior management concern as positively correlated with employees' knowledge-sharing behavior.

Assefa and Tensaye [10] highlight management support, training and awareness, and accountability as key organizational factors shaping employee compliance with existing information system security policies. Similarly, Alotaibi et al. [11] underscore the importance of training, awareness, and education in ensuring the effectiveness of information security policies, while also addressing challenges in their implementation.

In the competitive business environment, information is a critical resource for modern organizations, both internally and externally. Recognizing this importance, researchers have endeavored to identify general organizational factors influencing employee compliance with information system security policies. Alotaibi et al. [12] emphasized the indispensable role of training, awareness, and education in ensuring the effectiveness of information security policies. Their research underscores the necessity of addressing these factors to mitigate key challenges in successfully implementing information security policies.

3. Benefits Affecting to Share Knowledge

The process of knowledge sharing encompasses various activities, including acquiring new knowledge, applying it, preparing task-related information, collaborating with others, and generating ideas. This dynamic process occurs through continuous interaction among organizations, beneficiaries, and suppliers, fostering innovation [3]. Internal knowledge sharing occurs through regular meetings and informal discussions within the organization [1], while external sharing takes place through seminars and collaborative meetings with external entities. Participation in these activities enhances organizational efficiency and fosters better relationships with other enterprises, thereby improving overall information security.

- A strategic approach to knowledge management within an organization drives its advancement and growth, as collective collaboration forms the basis for generating new knowledge. This strategic approach not only enhances the organization's competitive advantage but also facilitates strategic alliances between enterprises. Increasing the organization's openness to knowledge management practices fosters knowledge exchange, enabling individuals to transform their knowledge into forms readily understandable and usable by others [12], thus addressing information security gaps effectively.
- Identifying and managing potential problems exemplifies good corporate governance practices [13]. This proactive approach benefits decision-making, performance, transparency, and the overall effectiveness of an organization's information security efforts by leveraging shared experiences and knowledge to address potential challenges [3].

- Sharing information, capabilities, and ideas across different domains can significantly enhance organizational capabilities and foster a culture of knowledge sharing. Leveraging experience and knowledge contributes to process development and enhances workforce competencies, leading to improved service quality, increased efficiency, and better utilization of technological resources. Conversely, the failure to foster a culture of knowledge sharing can lead to substantial financial losses for the organization [3].
- Utilizing knowledge sharing in information security reduces the cost of safeguarding organizational information and enhances awareness of information asset protection. Effective information systems play a crucial role in safeguarding organizational information by mitigating risks to its availability, confidentiality, and integrity. Increasing employee awareness of information confidentiality and security strengthens information security measures and support systems, consequently reducing information security costs [14].
- Sharing knowledge among employees enables a better understanding of cyber threats, facilitating proactive network protection measures. This includes early detection of covert cyberattacks, identification of new malware, issuance of early warnings, and dissemination of threat intelligence data. These efforts collectively mitigate the risks of information security breaches, underscoring the importance of employee adherence to organizational information security policies and procedures [3].

Sharing knowledge of information security has a positive impact on organizational employees, fostering collaboration in problem-solving, idea generation, policy implementation, decision-making, efficiency improvement, risk mitigation, cost reduction, and sharing of relevant experiences. Such knowledge sharing serves as a valuable resource in enhancing information security awareness [3].

4. Factors Affecting to Share Knowledge

Based on what was introduced earlier, information security knowledge sharing refers to working with others through the exchange of experience, ideas, and knowledge to protect information assets in an organization. Combined data, information, and human knowledge among employees is an asset that increases efficiency, reduces risk, and facilitates decision-making.

Knowledge sharing plays important role in an organization's information security governance. This has a positive impact on employee information security awareness. It is widely recognized as the key to preventing information security breaches in an organization. By sharing knowledge, we can avoid wasting time and unnecessary costs by developing the same solution for similar problems [14]. In other words, the effectiveness of information security knowledge sharing makes every organization aware of the importance of managing and improving knowledge among employees in an organization.

Sharing information security knowledge needs to pay attention to many aspects such as changing environmental conditions, human behaviors, and resource security [3]. Such awareness not only involves people's behavior but also their individual needs, privacy issues, trust concerns, and cultural thinking in the social environment [15]. Therefore, the awareness of exchanging knowledge among employees is affected and dependent on various factors. These are just a few that should be considered to significantly improve a company's operations by using sharing knowledge.

We group some factors into two broad categories: human behavior and organizational support, to share knowledge between employees.

2.1. Organization support

Our investigation into the effects of incentive factors on knowledge-sharing behavior within organizations revealed that employees' willingness to engage in knowledge-sharing is significantly influenced by the supportive capabilities of their organizations. Creating an environment conducive to knowledge-sharing requires organizations to cultivate the necessary skills and motivation among participants.

Organizational support encompasses the employees' overall perception of the organization's commitment to their well-being and the value placed on their contributions. This emotional commitment from employees is crucial, particularly in their adherence to information security policies. Numerous studies have demonstrated that employees are more inclined to

share knowledge when they perceive strong organizational support. This perception fosters a sense of commitment among employees, aligning them with organizational goals and policies, thereby safeguarding organizational information assets through effective knowledge-sharing mechanisms [14].

Another influential factor within organizations is organizational culture, which encompasses the values, beliefs, and systems that either encourage or hinder knowledge creation and sharing. Organizational culture manifests itself in both visible and invisible dimensions. The visible aspect includes the organization's espoused values, mission, and philosophy, while the invisible dimension consists of the norms and values guiding employee behavior and actions. A supportive organizational culture and positive relationships among employees can further motivate knowledge contribution [16].

Considering these factors, employees are more likely to engage in communication and knowledge-sharing related to security, fostering organizational commitment and a sense of responsibility for protecting information assets. This collaborative approach empowers employees beyond relying solely on IT security personnel.

2.2. Human behavers

The most influential factors driving knowledge-sharing behaviors are human behavior factors. Consequently, organizations concentrate on managing, modifying, and stimulating these behaviors. They tailor knowledge-sharing practices to their current circumstances and strive to foster effective behaviors among employees.

I. Motivations

Motivation encompasses the reasons behind people's actions, desires, and needs, shaping specific behavior patterns. Previous research indicates that motivations linked to individuals' needs and expectations can both encourage certain behaviors and influence their conduct. Employees' attitudes toward information security knowledge-sharing in organizations are significantly influenced by both intrinsic and extrinsic motivations, serving as drivers or determinants of knowledge-sharing behavior.

- Intrinsic motivation: This form of motivation is the most autonomous, driven by enjoyment and interest in the task itself or pleasure in assisting others. It originates from within the individual and is not reliant on external pressure or rewards. Intrinsically motivated individuals are more likely to enhance their capabilities and organizational productivity, as they demonstrate commitment to tasks, high work performance, and a drive to improve their skills.
- Extrinsic motivation: This type of motivation involves engaging in an activity to achieve a desired outcome, such as career advancement or monetary rewards, or to avoid social or material punishment. While weakly associated with work performance and effort, extrinsic motivation is often linked to perceptions of costs (effort) and benefits (rewards) associated with sharing knowledge. Many organizations implement reward systems to incentivize employees to share knowledge [14].

Work design characteristics may influence the motivation to share knowledge with colleagues. Furthermore, knowledge sharing and hiding may stem from different motivations.

II. Intention

Intention involves planning and mental activity aimed at achieving a goal. It is a concept widely studied in the domain of information security behavior, including intentions to comply with organizational policies, adopt security behaviors, exhibit IT ethical behavior, and engage in information security knowledge sharing [14]. Consequently, the intention to share information security knowledge significantly influences employees' behaviors and motivations in this regard.

III. Trust

Trust entails a belief in the honesty, dependability, goodness, and effectiveness of someone or something. It is crucial in interpersonal relationships and social systems, fostering knowledge sharing among individuals. Factors such as trust in the recipient of information and face-to-face interactions contribute to increasing motivation for knowledge sharing [19]. However, trust can also be a barrier, as Information Security Administrations may refrain from sharing information due to concerns about potential misuse by attackers [14]. Trust remains a cornerstone in the realm of information security knowledge sharing.

In conclusion, these factors collectively impact knowledge sharing among employees, particularly in the context of information security. Companies must support behaviors conducive to knowledge sharing to influence organizational objectives and policies positively. Management plays a crucial role in fostering and enhancing information security knowledge sharing by motivating staff, increasing intention and trust, and providing organizational support, ultimately mitigating the risk of information security breaches.

5. Barriers to Share Knowledge

Undoubtedly, sharing knowledge in information security faces numerous barriers that hinder its dissemination among organizations and employees.

The primary obstacle stems from the low level of awareness and understanding of information security protocols and sharing mechanisms among both internal employees and external organizational partners [3]. In both public and private sectors, several challenges hinder information sharing from various perspectives [19]. Moreover, the absence of a clear strategy and defined work objectives exacerbates barriers to knowledge sharing [16].

The human factor emerges as the most significant barrier to knowledge sharing. Further investigation into these factors is essential to establishing and strengthening relationships conducive to knowledge sharing in information security [19].

Confidentiality breaches represent a major barrier, as employees may inadvertently share sensitive information, leading to potential harm to individuals or organizations. Such breaches instill fear and reluctance in individuals, impeding further knowledge sharing [20].

Concerns about violating privacy also deter participation in knowledge-sharing activities. Research suggests that employees withhold information if they perceive a risk of losing competitive advantage [18]. Additionally, cultural differences can influence the willingness to share knowledge [18]. To address this challenge, managers can allocate specific time for knowledge exchange during work hours or incentivize sharing through rewards such as additional vacation days. Such measures foster a culture of knowledge sharing and enhance organizational performance [21].

Regardless of the type of knowledge being shared, lack of motivation poses a significant barrier to knowledge-sharing behavior. Studies have identified low willingness or intention among members to share knowledge as a crucial obstacle to information security knowledge sharing [14] [22].

6. Conclusion

Knowledge sharing plays a vital role in advancing organizational objectives and distinguishing companies through enhanced capabilities and benefits. Facilitating the exchange of knowledge among employees proves to be a cost-effective method for elevating their competencies, aligning with the overarching goal of establishing a secure environment for information assets. Management's support for such activities significantly enhances collaboration on information security, thereby mitigating the risk of breaches.

Governance initiatives further bolster information security sharing within enterprises by delineating policies that articulate the organization's intent and values regarding knowledge contribution. Management bears the responsibility of fostering an environment conducive to knowledge exchange, motivating employees to participate actively, and ensuring awareness of information security importance and guidelines among staff.

Our research underscores the significant impact of motivational factors on attitudes toward knowledge-sharing behavior in the realm of information security. To enhance information security knowledge sharing, management can leverage intrinsic and extrinsic motivations, recognizing that intrinsic motivation stems from personal interest or satisfaction in the task, while extrinsic motivation originates from external influences. Additionally, fostering intention and trust among employees enhances knowledge-sharing practices.

Identified barriers, including concerns about confidentiality, sensitive information, privacy violations, competitive advantage, lack of motivation, and low willingness or intention, hinder effective information and knowledge exchange within organizations.

We advocate for the consideration of organizational aspects of information security by academics and practitioners alike. This includes emphasizing information security knowledge sharing, adherence to information security policies, and procedures to ensure comprehensive safeguarding of organizational assets.

References

[1] Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. International Journal of Information Management, 36(2), 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

[2] AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges AND CRITICAL SUCCESS FACTORS: Systematic review. Computers & Security, 99, 102030. https://doi.org/10.1016/j.cose.2020.102030

[3] Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. Computers & Security, 56, 70–82. https://doi.org/10.1016/j.cose.2015.10.006

[4] Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. Computers & Security, 60, 154–176. https://doi.org/10.1016/j.cose.2016.04.003

[5] Jen, C. T., Hu, J., Zheng, J., & Xiao, L. L. (2019). The impacts of corporate governance mechanisms on knowledge sharing and supply chain performance. International Journal of Logistics Research and Applications, 23(4), 337–353. https://doi.org/10.1080/13675567.2019.1691515

[6] Goffnett, S. P., & Williams, Z. (2018). The path between supply chain efficacy and performance: Testing a secure route. International Journal of Logistics Research and Applications, 22(1), 98–117. https://doi.org/10.1080/13675567.2018.1475555

[7] Charterina, J., Landeta, J., & Basterretxea, I. (2017). Mediation effects of trust and contracts on knowledge-sharing and product innovation. European Journal of Innovation Management, 21(2), 274–293. https://doi.org/10.1108/ejim-03-2017-0030

[8] Sohrabi Safa, N., Maple, C., Watson, T., & Furnell, S. (2018). Information Security Collaboration Formation in organisations. IET Information Security, 12(3), 238–245. https://doi.org/10.1049/iet-ifs.2017.0257

[9] Xuan, V. N. (2020). Factors affecting knowledge sharing in enterprises: Evidence from small and medium enterprises in Vietnam. Management Science Letters, 469–478. https://doi.org/10.5267/j.msl.2019.8.023

[10] Assefa, T., & Tensaye, A. (2021). Factors influencing information security compliance: An institutional perspective. SINET: Ethiopian Journal of Science, 44(1), 108–118. https://doi.org/10.4314/sinet.v44i1.10

[11] Alotaibi, M., Furnell, S., & Clarke, N. (2016). Information security policies: A review of challenges and influencing factors. 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST). https://doi.org/10.1109/icitst.2016.7856729

[12] Santoro, G., Vrontis, D., Thrassou, A., & Dezi, L. (2018). The internet of things: Building a knowledge management system for open innovation and Knowledge Management Capacity. Technological Forecasting and Social Change, 136, 347–354. https://doi.org/10.1016/j.techfore.2017.02.034

[13] Zeeshan, A. K., & Kristin, A. (2018). Information security risk management practices: Community-based Knowledge Sharing. Retrieved January 18, 2023, from https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2568034

[14] Safa, N. S., & Von Solms, R. (2016). An information security knowledge sharing model in organizations. Computers in Human Behavior, 57, 442–451. https://doi.org/10.1016/j.chb.2015.12.037

[15] Diesch, R., Pfaff, M., & Krcmar, H. (2020). A comprehensive model of information security factors for decision-makers. Computers & Security, 92, 101747. https://doi.org/10.1016/j.cose.2020.101747

[16] Razmerita, L., Kirchner, K., & Nielsen, P. (2016). What factors influence knowledge sharing in organizations? A social dilemma perspective of social media communication. Journal of Knowledge Management, 20(6), 1225–1246. https://doi.org/10.1108/jkm-03-2016-0112

[17] Gagné, M., Tian, A. W., Soo, C., Zhang, B., Ho, K. S., & Hosszu, K. (2019). Different motivations for knowledge sharing and hiding: The role of Motivating Work Design. Journal of Organizational Behavior, 40(7), 783–799. https://doi.org/10.1002/job.2364

[18] Agrawal, V., & Snekkenes, E. A. (2017). Factors affecting the willingness to share knowledge in the of practice. Lecture Notes in Computer Science, 32–39. https://doi.org/10.1007/978-3-319-63874-4_3

[19] CARR, M. A. D. E. L. I. N. E. (2016). Public-private partnerships in national cyber-security strategies. International Affairs, 92(1), 43–62. https://doi.org/10.1111/1468-2346.12504

[20] Bari, M. W., Ghaffar, M., & Ahmad, B. (2020). Knowledge-hiding behaviors and employees' silence: Mediating role of psychological contract breach. Journal of Knowledge Management, 24(9), 2171–2194. https://doi.org/10.1108/jkm-02-2020-0149

[21] Topa, I., & Karyda, M. (2019). From theory to practice: Guidelines for Enhancing Information Security Management. Information & Computer Security, 27(3), 326–342. https://doi.org/10.1108/ics-09-2018-0108

[22] Serenko, A., & Bontis, N. (2016). Understanding counterproductive knowledge behavior: Antecedents and consequences of intra-organizational knowledge hiding. Journal of Knowledge Management, 20(6), 1199–1224. https://doi.org/10.1108/jkm-05-2016-0203