Research on Information Security Issues and Countermeasures in the Era of Digital Intelligence Organizational Development

Xue Chen, Guiqin Li*

School of Management, Chengdu University of Information Technology, Chengdu, 610103, P.R.China

chen0129.cx@qq.com, *e2001011@163.com

Abstract. In the era of widespread big data and artificial intelligence, economic development and social progress have accelerated. However, along with rapid growth, the openness of networks has brought about certain drawbacks, such as increased information security risks within organizations, including technical vulnerabilities, virus invasions, and human errors. Ensuring the security, stability, and continuity of enterprise operations becomes paramount. This article employs literature analysis and comparative analysis methods to explore the hidden risks of information security within organizations. It proposes corresponding countermeasures from technological, managerial, human, and environmental perspectives, providing theoretical support for the sustainable and healthy development of relevant enterprises.

Keywords: Big data, Artificial Intelligence, Information Security, Organizational Development.

1 Introduction

Currently, with the rapid development of information technology and artificial intelligence, we are fully immersed in the era of big data and artificial intelligence, where digital intelligence drives national development, brings benefits to organizations, and facilitates people's lives. However, information security issues have emerged as by-products of this era. Information security involves the confidentiality, integrity, and availability of information, aiming to protect all data, including information technology security, data security, content security, and behavioral security [1]. In recent years, information security issues have become increasingly prominent, posing serious threats to organizations of all sizes in China. For example, there is a concern that malicious actors may exploit ChatGPT to create phishing websites and develop illegal apps, leading to deception, unauthorized registration, and fraudulent activities[2].Therefore, the importance of information security has become unprecedented. This article aims to discuss the current information security challenges faced by organizations and explore effective preventative measures and responses. Based on different types of information

L. Chang et al. (eds.), *Proceedings of the 2024 8th International Seminar on Education, Management and Social Sciences (ISEMSS 2024)*, Advances in Social Science, Education and Humanities Research 867,
https://doi.org/10.2991/978-2-38476-297-2_97

security issues, this study comprehensively reviews the existing information security problems within organizations and proposes an optimized path for future organizational information security governance.

2 Information Security Status

2.1 Current Status of Domestic Research

Scholar Li Xueshi was among the earliest to propose the concept of information security, enriching its meaning from a confidentiality perspective. Feng Dengguo has highlighted that with the widespread use of the internet, users' information security is at risk, as their information can be firmly controlled by businesses. Therefore, issues of security and privacy are particularly important. Nowadays, research on information security in China is becoming increasingly rich and diverse. There is a growing emphasis on areas such as cybersecurity, data protection, network defense, privacy preservation, and secure communication. Researchers are exploring advanced technologies like blockchain, artificial intelligence, and quantum cryptography to enhance information security measures. Academic institutions, government agencies, and industry are actively collaborating to promote research, knowledge exchange, and the development of practical solutions to address the evolving challenges in information security. In this paper, "information security" is searched by CNKI. Research mainly focuses on computer software, computer applications, and internet technologies. The research directions primarily revolve around (1) the study of information security literacy, (2) research on information security technologies, (3) research on information security behavior, and (4) research on information security protection.

2.2 Current Situation of Foreign Research

In the 1950s, Hans J. Morgenthau, a renowned international relations theorist in the United States, wrote in "Politics Among Nations": "Information technology brings various advantages to national governments, but also poses significant risks and challenges to national security" [3]. According to researchers such as Lena Y. Connolly et al., they conducted semi-structured interviews to collect data on the influence of national culture on employees' attitudes and behaviors towards information security in Ireland and the United States. The survey findings reveal that, within the observed organizations, American employees are more inclined to adopt formal information security policies and procedures compared to Irish employees[4]. Scholars such as Pataci et al. examined the influence of organizational information security risk perception on boundary change behavior using theories of organizational behavior and traditional risk management approaches. The study found a positive correlation between organizational information security risk perception and risk transfer behavior, as well as low-risk boundary change behavior[5].In this study, a search was conducted using the Web of Science database for "information security". From a timeline perspective, foreign research on information security began early, tracing back to the early 20th century. Research in foreign countries primarily focuses on computer science, engineering, and telecommunications.

On one hand, foreign research examines employee information security behavior from an organizational perspective. Guhr and others conducted research on the information security participation intentions of organizational employees and leaders, highlighting the decisive role of organizational leadership in employees' information security behavior [6]. On the other hand, some scholars approach the study of user information security behavior from a behavioral theory perspective. Eirik believes that motivation has a significant impact on users' information security awareness [7].

3 Information Security Issues in the Era of Digital Intelligence

3.1 Technical Vulnerabilities

The main cause of information leakage is insufficient security measures in information systems. Many small and medium-sized enterprises have vulnerabilities in their information systems due to limited funds or manpower. With the development of artificial intelligence technology, numerous AI products have emerged. For example, ChatGPT, which gained popularity online from late 2022 to early 2023. It increases the risk of data security. The way users interact with ChatGPT turns their inputted information into iterative data. If personal information is inputted, ChatGPT may inadvertently output it as an answer to others. Furthermore, if ChatGPT's system has vulnerabilities and falls victim to attacks, large amounts of user data and information can be stolen. For instance, after Samsung introduced ChatGPT, there were three incidents of device information and meeting content leaks, resulting in irreversible losses.

3.2 Negligence at the Management Level

In addition to technical vulnerabilities, the lack of attention from the management level within organizations is another important factor. This is especially true for small and medium-sized enterprises, as they often fail to keep their policies and governance in sync with national policies. Most small and medium-sized enterprises lack comprehensive information security management and fail to establish their own information security guidelines. These companies often cut corners in information security training and do not have dedicated information security positions, leading to a lack of preparedness for contingencies. Once an information security incident occurs, the losses can be devastating. Research shows that the attention given by management has a positive correlation with the healthy development of information security within organizations. For example, Guhr and others conducted research on the information security participation intentions of organizational employees and leaders, highlighting the decisive role of organizational leadership in employees' information security behavior [6]. Liu Chenhui and Wang Nengmin conducted a survey to explore the impact of organizational control on information security compliance behavior, and reveal that organizational commitment has a significant positive effect on information security compliance behavior [8].

3.3 Interference from Human Factors

Research by the United States Computer Crime and Security Investigation Bureau indicates that human factors account for 52% of the causes of network security incidents. In the early 1990s, scholars such as C. Wood were among the first to pay attention to the human factors in information security, pointing out that human factors have a certain latent impact on information system security [9]. Schultz E. (2005) proposed that information security is primarily a human issue rather than a technical issue [10]. A series of studies have shown that whether employees comply with regulations is a major part of information security. In 2018, Facebook suffered a serious data breach when Cambridge Analytica, a data analytics company, collected personal information from nearly 90 million Facebook users. Not only did they obtain information from users who used the application, but they also obtained information from their friends' lists, resulting in the leakage of information from 87 million Facebook users. More and more researchers have gradually realized the importance of human factors in information security, as they represent a significant and uncertain aspect of information security protection.

4 Measures for Preventing Information Security Risks

4.1 Strengthen Technical Protection

Information leakage is the most common security risk for enterprises. Regardless of the organization's size, it is essential to implement robust network security defense measures, such as using firewalls, intrusion detection and defense systems, and antivirus software to monitor and prevent potential network attacks. Strategies and methods to prevent information leakage from a technical perspective mainly include strengthening data encryption and permission management. Technical protection can prevent the leakage of critical data from the source, making it an effective and feasible information security measure. Firstly, strengthening data encryption is an important means to prevent information leakage. Data should be encrypted during transmission, storage, and processing to ensure that even if the data is illicitly obtained, it cannot be deciphered. Secondly, permission management is an effective means of controlling information access. Establishing a detailed permission management system ensures that only authorized users can access relevant data, effectively reducing incidents at the source.

4.2 Enhance Security Management

(1)Improve Employee Security Awareness.

As mentioned earlier, human factors are a major and important cause of information leakage. Therefore, preventing information leakage and ensuring information security requires addressing the human factor. Employees are vital to the smooth operation of an organization, and their behavior is closely linked to the interests of the organization. Improper employee operations, whether intentional or unintentional, can expose organizations to information security attacks. To mitigate potential risks associated with

human factors, organizations should provide appropriate guidance and training to relevant personnel, including systematic training and testing upon joining the organization.

(2)Emphasize Network Security Management.

In the era of big data and artificial intelligence, communication between individuals has become more convenient, and the speed and scope of information dissemination have increased. Managers need to possess professional knowledge of information security and adopt practical management methods. They should communicate information security management regulations to personnel in a timely manner and constrain their information security behavior. Organizations should pay attention to hiring individuals who prioritize information security awareness, and once they join the organization, their operations should be regulated and unified information security standards should be established and enforced.

4.3 Strengthen Regulatory Compliance

Various new information technologies and application patterns emerge constantly, while the corresponding laws and regulations lag behind, leading to legal gaps or difficulties in application. Some laws and regulations have broad and abstract descriptions in specific terms, resulting in significant flexibility in practical execution, which can be abused. Companies deal with a large number of information subjects, yet the protection of the rights and interests of these subjects is insufficient under the current legal framework. The reasons for legal issues can be summarized as follows: firstly, the continuous emergence of emerging technologies outpaces the update of laws and regulations. Secondly, the enforcement of laws and regulations is insufficient, resulting in inadequate persuasive power for some laws and regulations.

5 Conclusion

This paper has strong theoretical and practical significance for the healthy development of organizations. This paper introduces various information security issues in organizational development, such as technical vulnerabilities, negligence at the management level, and employee unsafe behavior. It provides guidance on preventive measures for these issues, emphasizing the importance of continuous attention to information security in the era of big data and artificial intelligence. Strengthening technical protection, enhancing regulatory supervision, improving employee awareness of information security.

Acknowledgments

This paper is financially supported by the National Social Science Fund of China (Grant Number 19BGL123) and the Chengdu University of Information and Technology Innovation Capacity Enhancement Program (Grant Number KYTD202229).

References

1. LiuXianquan. The Impact of Generative Artificial Intelligence on the Data Privacy and Criminal Law Protection System. [J].Chinese Journal of Criminal Law, 2023(4):20-34.
2. PU Qingping, XIANG Wang. Opportunities and challenges aroused by ChatGPT as generative AI and strategy for response[J]. Journal of Chongqing University(Social Science Edition), 2023, 29(3): 102-114.
3. Hussein R, Lambensa F, Anom R. Information security behaviour: A descriptive analysis on a Malaysian Public University [EB /OL]. [2014 - 12 - 23]. eprints. sunway. edu. my /114 /1 / ICS2011 _ 14. Pdf.
4. Connolly L Y, Lang M, Wall D S. Information security behavior: A cross-cultural comparison of Irish and US employees[J]. Information Systems Management, 2019, 36(4): 306-322.
5. Pataci H, Ravichandran T. Information Security Risk Perception and Firm Behaviour[C]// Academy of Management Proceedings. Briarcliff Manor, NY 10510: Academy of Management, 2022, 2022(1): 18261.
6. Guhr N, Lebek B, Breitner M H.The impact of leadership on employees'intendedinformation security behaviour:An examination of the full-range leadership theory[J].Information Systems Journal,2017,29(2):340-62.
7. Albrechtsen E.A qualitative study of users'view on information security[J].Computersand Security,2007.
8. Liu Chenhui, Wang Nengmin. The Impact of Organizational Control on Information Security Compliance Behavior: The Moderating Effects of Supervisor-Subordinate Guanxi and Organizational Commitment[J]. Management Review, 2022, 34(9): 208-220.
9. Wood C, Jr. Banks W. Human error: An overlook but significant information security problem[J]. Computers &Security, 1993, 12 (1): 51 - 60.
10. hultz E. The human factor in security[J]. Computers and Security, 2005, 24(6) : 425 - 426.