менеджерлерге тілдік түсініспеушіліктерді азайту, ақпаратты нақты жеткізу және қызметкерлерге ашық, сенімді қарым-қатынас орнату маңызды.

Коммуникация – менеджменттегі ең маңызды құралдардың бірі. Ол ұйымның тиімді жұмыс істеуін қамтамасыз етіп, басшылық пен қызметкерлер арасындағы байланыс процесін реттейді. Тиімді коммуникация жүйесі ұйымның дамуына, қызметкерлердің ынтасын арттыруға және жалпы өнімділікті жақсартуға мүмкіндік береді.

Менеджменттегі коммуникация ұйымның сәтті және тиімді жұмыс істеуінде аса маңызды рөл атқарады. Ол ақпарат алмасуды, шешімдерді уақытында қабылдауды және жұмыс процесін үйлестіруді қамтамасыз етеді. Тиімді коммуникацияның арқасында басшылар мен қызметкерлер арасында түсіністік орнап, ұйым ішіндегі процестердің үйлесімділігі артады.

Негізінен, коммуникация – ұйымның тірегі. Егер ұйымдағы ақпарат алмасу дұрыс ұйымдастырылмаса, өнімділік төмендеп, қызметкерлердің ынтасы әлсіреуі мүмкін. Сол себепті кез келген басшы үшін коммуникация дағдыларын жетілдіру және оны дұрыс ұйымдастыру – табысты басқарудың басты шарты.

Әдебиеттер тізімі

1. Роберт Л. Кац, “Менеджменттің негізгі функциялары”
2. Мескон, Альберт, Хедоури- Менеджмент негіздері”
3. https://www.kaznu.kz/content/files/pages/folder21049/%D2%9A%D0%B0%D0%B9%D1%80%D0%B0%D1%82%D0%BE%D0%B2%D0%B0%205.pd
4. KAZ Minerals | Главная

Challenges for corporate governance in the digital age: new risks of data loss and privacy.

N. B. Davletbayeva [1], T.A. Nurseit[2], Z. S. Takuova[3]

[1]Candidate of Economic Sciences of the Non-Profit Joint Stock Company Karaganda Buketov University

[2]Master's student of the Management Department of the Non-Profit Joint Stock Company Karaganda Buketov University

[3]Master of Education in Pedagogical Sciences Non-Profit Joint Stock Company Karaganda Buketov University

n.davletbaeva74@mail.ru , torgyn.nurseit@gmail.com, zarinchen@mail.ru

Karaganda Buketov University, Karaganda

Abstract: The article "Challenges for corporate governance in the digital age: new risks of data loss and privacy" discusses the major issues related to data loss management and privacy violation management, considering the digital transformation of the Kazakhstani economy. The group emphasizes that detailed risk management approaches should be developed by analyzing modern risks such as cyberattacks, data leaks, and a lack of awareness among staff members. Particular consideration is given to the application of contemporary technology, such as blockchain and artificial intelligence, employee training, and the application of international standards like ISO 27001. In conclusion, the authors emphasize the strengthening of the regulatory framework, the necessity of intersectoral cooperation for improving the sustainability of the digital economy. The recommendations deal with the implementation of the information security management systems, the creation of national plans in order to reduce the risks and create a competitive economy.

Keywords: Digital transformation, data loss, data confidentiality, risk management, cybersecurity, artificial intelligence, digital economy, information security, corporate governance, cyberattacks, regulatory compliance

Today, the world is experiencing new perspectives of digitalization leading to its transformation in varied spheres of economics and social life. In particular, the digitalization process in Kazakhstan has become a basic priority in the government policy aimed at fostering economic development and

competitiveness. The national programs, including Digital Kazakhstan' and The Concept of digital transformation, development of ICT industry and information security provision by 2026, Gov. Decree RK No.269 of 03/28/2023, create a system of incentives for the introduction of innovative technologies and stimulation of business development in new conditions. On the other hand, the faster advancement in the field of digital economy comes with a greater risk level as well, for instance, in the context of data loss and the breach of information secrecy.

As organizations continue to operate in a digital environment, issues of data security and privacy are gaining more relevance. The fact that information can damage a company's reputation, along with causing financial loss, is a major worry in today's competitive market. Citing the Committee on Statistics of Kazakhstan, there has been an increase in cyber attacks on businesses in the finance and technological fields. The significance of establishing efficient risk management mechanisms is found within that. In the digital economy, today's boards and managers must reassess their perspectives on security. Developers and suppliers of cloud services, as well as AI and large data sets, make it more challenging to oversee information flows. Yet, the situation is exacerbated by the lack of a sufficient number of skilled experts and proper legal guidelines.

In this study, therefore we want to focus on the major concerns that businesses consider incorporating some measures aimed on improvement of their corporate governance with respect to these threats in the economy of Kazakhstan in the current scenario context of digitalisation. Their management styles that incorporate core factors that handle these risks effectively will also be demonstrated.

One of the greatest risks to the digital economy is the loss of data and that related to privacy. In the sphere of digitalization, data has become a core resource and its security has its own set of risks. Data occurrence may be due to outside threats such as cyber-attacks, virus programs and phishing, or self-inflicted internal damage as in the case of employees making mistakes or malfeasance. Other factors such as equipment failure, absence of redundancy and use of obsolete tools tend to aggravate those risks. The term "data confidentiality" refers to the prevention of sensitive information from being disclosed to unauthorized persons. This is becoming increasingly difficult as the volume of data that needs to be managed increases with the introduction of cloud computing services.

Other dangers in Kazakhstan come from employees not being well-informed, lack of investment in information security, and inability to follow international standards. For example, in 2023, a leak of customer data from a telecommunications company sparked concerns and raised doubts about the company. It is worth noting that in February 2024, there were also reports of data on the health statuses of Al-Farabi University students in Almaty being leaked. This occurrence has surfaced as a troubling example of breaches in educational institutions, exposing weaknesses in privacy protection. An integrated strategy is needed to reduce these risks, which includes developing regulatory requirements, training employees, and implementing information security management systems.

Digital transformation now makes part of the economic strategy of Kazakhstan to boost competitiveness and invite investments. The state program "Digital Kazakhstan" approved by Gov. Decree RK dated 12.12.2017 NO. 827 and the "Concept of digital transformation, development of the information and communication technology industry and information security till 2026" Gov. Decree RK dated 28th March 2023 Vol.269 lays down the framework for the risks inherent in the process. Nonetheless, the integration of digital technologies into the economy is hindered by substantial risks, as detailed in the papers. As per the National Cybersecurity Center, in 2022, there was a thirty percent rise in cyber-attacks targeting Kazakhstani companies, including those in the education sector. In January 2023, there were 4.2 thousand cyber-attacks in the country, which is double the number of cyber-attacks from the same period in the previous year, as stated in February 2024.The issue of loss of data is also of great importance to the educational sector as well as to small and medium enterprises who do not have adequate enough facilities to shore up for information security.

The Republic of Kazakhstan's "On Personal Data and their Protection" law from 07/05/2024 regulates how personal information is processed and stored, contributing to safeguarding data under the country's legal system. Nevertheless, with insufficient government oversight and corporate

knowledge of existing laws, the level of implementation remains low. For example, many companies do not implement routine data backups, leaving them vulnerable to external risks. Additionally, the problem is exacerbated by the shortage of cybersecurity and IT professionals, leading to challenges in adopting global standards. Within the digital transformation landscape, these factors emphasize the importance of adopting a unified strategy for managing risks. The experience of Kazakhstan shows that an important way to improve sustainability could be to develop national information security strategies, involving training for employees, the implementation of modern technologies, and the improvement of regulations.

The economy of Kazakhstan is increasingly going digital, raising important concerns about data security and confidentiality in corporate management. One of the primary problems is the lack of experienced information security experts. Many businesses are struggling to find workers with the necessary skills due to the use of advanced technology and the growing amount of data. The lack of skills puts companies at risk of cyber-attacks, damaging the confidence of customers and partners.

Adapting to changing regulations is also a significant challenge. Despite the presence of the law "On Personal Data and their protection," it is often enforced in a superficial way and oversight of compliance is lacking. Many small and medium-sized companies connect compliance with increased spending on technology and staff training.

Adapting to changing regulatory requirements is also a significant challenge. Although the law regarding "Personal Data and their protection" is in place, it is often enforced in a superficial way and lacks sufficient monitoring for compliance. Most small and medium-sized enterprises connect compliance with increased technology and staff training costs.

To effectively address the risks of data loss and confidentiality, it is essential to take a holistic approach by utilizing advanced technologies, enhancing internal procedures, and increasing employee knowledge. In Kazakhstan, incorporating information security management systems (ISMS) is increasingly crucial for reducing risks. These systems enable the detection and prevention of possible risks to ensure the safeguarding of essential data.

Utilizing blockchain technology is a highly effective method for managing risk. The high level of data safety is provided by its decentralized architecture and encryption techniques. For example, companies in the banking sector of Kazakhstan are starting to implement blockchain technology to secure transactions and enhance transaction visibility.

Employee training is also an essential tool. Due to human mistakes being responsible for most data breaches, regular cybersecurity training and educating employees on current threats have become crucial aspects of risk mitigation. For example, companies can conduct phishing attack simulations to increase employee knowledge.

Data backup and highly secure cloud solutions also reduce the impact of technological malfunctions and cyberattacks. An example of this is that large companies in Kazakhstan are already leveraging secure and flexible hybrid cloud solutions.

The incorporation of international standards like ISO 27001 "Information Technology" is also essential for successful risk management. These guidelines offer precise information security advice, which is crucial for businesses doing business internationally. The adoption of these standards is growing in popularity among big businesses in Kazakhstan.

Finally, businesses can anticipate potential risks and take preventative action by utilizing analytical tools built on artificial intelligence. These techniques have already demonstrated their efficacy in global practice and hold great promise for use in Kazakhstan.

Adopting global benchmarks such as ISO 27001 "Information Technology" is crucial for effective risk management. This advice provides important information security recommendations that are essential for businesses operating on a global scale. Big businesses in Kazakhstan are increasingly favoring the adoption of these standards.

Finally, companies can use AI-based analytical tools to predict risks and proactively mitigate them. These methods have proven effective on a worldwide scale and show potential for implementation in Kazakhstan.

Kazakhstan needs to develop and implement thorough policies at both the government and organizational levels to minimize the chances of data loss and breaches of confidentiality in the digital economy. Developing a national strategy for managing information security, including specific standards, business requirements, and monitoring mechanisms, is essential. This method should be consistent with international standards such as the NIST Cybersecurity Framework and ISO 27001 Information Technology guidelines.

Businesses need to prioritize employee training because human error remains a significant factor in data leaks. Regular trainings, seminars, and cyberattack simulations will enhance staff awareness of current threats. Implementing a security policy that outlines how to use company resources and controls data access can significantly reduce risks.

Another crucial step is technological rejuvenation. Modern tools including security monitoring programs, encryption tools, and access control systems should be used by businesses. For instance, using hybrid cloud technology increases data management flexibility and threat resilience.

The legislative framework needs to be strengthened at the state level. The Republic of Kazakhstan's "On Personal data and their protection" law must be completed to enforce more stringent standards compliance and hold businesses more accountable for data breaches. The establishment of specialist organizations to keep an eye on and address cyber occurrences can help increase the country's economy's resistance to dangers.

Establishing collaborations between the government, industry, and academic institutions to develop information security experts is also a crucial topic. Universities in Kazakhstan ought to create curricula that address the demands of the modern digital economy.

Lastly, businesses ought to aggressively deploy AI and machine learning-based threat early warning systems. With the use of these technologies, potential assaults can be anticipated, and preventative action can be taken quickly. Businesses in Kazakhstan have already begun incorporating these solutions, creating opportunities to raise the standard of data security.

The adoption of global standards like ISO 27001 "Information Technology" and the incorporation of cutting-edge technologies like blockchain and artificial intelligence require particular consideration. In addition to reducing risks, these solutions can help Kazakhstan build a competitive and sustainable digital economy.

Collaboration with the government, industry, and educational institutions is required to accomplish these objectives. The only way to reduce the dangers of data loss and guarantee confidentiality—the cornerstones of establishing confidence in the digital age—is to work together to create favorable conditions. This study emphasizes the necessity of a strategic approach to data management, which is especially crucial for Kazakhstan's economic growth and integration into the international digital economy.

References

1 Gusarova A., Dzhaksylykov S. Personal data protection in Kazakhstan: status, risks and opportunities // Soros Foundation-Kazakhstan. - 2020. – 52 p.

2 Akhmetova S. Some aspects of legislation on personal data protection // Kazakhstan Bar Association. – 2022

3 Uralova D. J. Problems of the risk management system at enterprises in Kazakhstan and the specifics of their improvement // Young Scientist. – 2016. – №10 (114). – Pp. 908-911

4 The Law of the Republic of Kazakhstan "On Personal Data and their Protection" (dated 07/05/2024) – The official text is available on the government portal of Kazakhstan: adilet.zan.kz.

5Committee on Statistics of Kazakhstan – Reports on cyber attacks on companies and organizations in the Republic of Kazakhstan. Data on cyber attacks can be found on the website: stat.gov.kz

6 Reports of the National Cybersecurity Center of Kazakhstan – Data on the increase in the number of cyber attacks in Kazakhstan. Information is available on the website: www.gov.kz.