Analysis and assessment of information security risks for sustainable development of the oil and gas industry

Mariia Maslova[1,2*]

[1]Sevastopol State University, 33, University str., Sevastopol, 299053, Russia
[2]Rostov State University of Economics (RINH), 69, Bolshaya Sadovaya str., Rostov-on-Don, 344002, Russia

Abstract. The problem of ever-evolving and growing risks never ceases to be an issue. Organizations in the oil and gas industry need to spend more and more money on protection, look for more qualified workers or train their staff on various innovations in this field. After many foreign vendors left the Russian market due to sanctions, threats that were minor have become more dangerous. Since even the most common risk in the form of, for example, a phishing link can become a big problem if it is partially disabled or there is no full protection of the functionality. Therefore, it is necessary to create their own software, their own methods of assessing risk events in information security, which will correspond to different areas of risk situations and at the same time have the quality of services, good functionality, not high cost and excellent quality. This article discusses a new unified method of information security containing the positive qualities of other methods and standards for assessing information security risks, but with the elimination of their shortcomings with the possibility of application in organizations of the oil and gas industry.

1 Introduction

In today's rapidly evolving digital environment, ensuring the security of confidential information is of paramount importance for organizations of all sizes. To address this critical task, a new approach has been developed that includes a wide range of techniques and standards for identifying and analyzing information security risks. This comprehensive method not only assesses risks, but also provides actionable recommendations for mitigating and eliminating them [1-5]. As businesses become increasingly dependent on the Internet of Things (IoT), the need for information security is growing. The Internet of Things is defined as a cyber-physical ecosystem of interconnected sensors and actuators that make it possible to make decisions [6-10]. The concept of the Internet of Things was part of our lives for several decades before the term became popular. Until the 2010s, several sectors of society used IoT devices and applications, but on a small scale. It offers users the ability to integrate devices, data and applications using Internet protocols. Consequently, many researchers have

* Corresponding author: mashechka-81@mail.ru

been working on an overview of the Internet of Things to gain knowledge about the Internet of Things ecosystem and its details. Several works have been done to give a general idea of the problems faced by the Internet of Things. Decision makers must take its protection seriously [3, 11]. Physical security protects employees, facilities, and assets from credible threats. These threats can come from internal or external attackers who compromise the security of data.

Developed to protect information from various threats, comprehensive information protection systems are used in various fields such as government, finance, healthcare and others. The essence of a comprehensive information protection system is to combine various information protection methods and technology into a single system that allows for comprehensive data protection [12].

An important aspect of developing an integrated information protection system is to analyze the risks associated with a particular system and develop appropriate protection measures to minimize those risks. Security risk assessment and risk management processes are the foundation of any security management strategy, as they provide a detailed understanding of the threats and vulnerabilities that can lead to financial damage to a business and how they should be addressed. It is also important to consider modern information security threats and ensure that data is protected against them accordingly [4]. Comprehensive information security systems are used to protect critical information such as state secrets, personal data, financial data, and others. They allow to provide reliable data protection and prevent information leaks, which is an important aspect of information security.

2 A comprehensive approach to improving information security

When developing the new method, a careful selection of different methodologies and standards was made. These include such well-established systems as MOF risk management, CRAMM, RiskWatch, MSAT, Microsoft, FRAP, GRIF, Risk IT, STO BR IBBS, SORAS, ISO/IEC 27001, OCTAVE, FSTEC and BS 7799 (Figure 1).

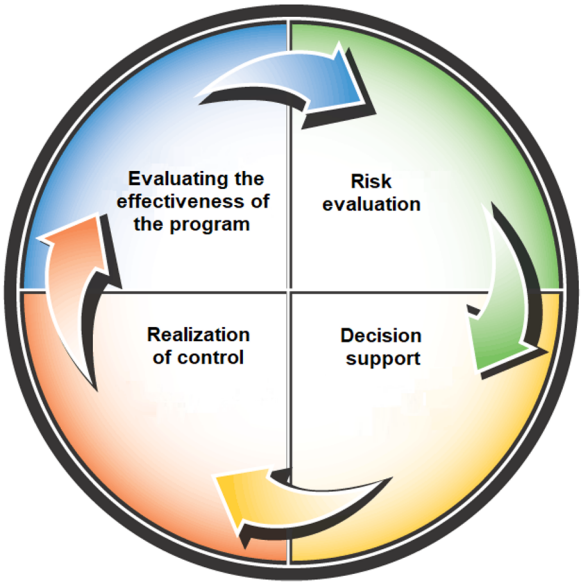

Fig. 1. Risk management process.

This diverse set of tools is the foundation for establishing a robust information security risk assessment process.

Creating a precise list of required protection measures depends largely on the needs of the company. The more valuable the equipment or data is, the more steps need to be taken to protect it. There are many different security systems available. However, before implementing any of them, the full range of possible scenarios should be analyzed as thoroughly as possible.

Proper security analysis helps demonstrate to the management team that evidence, not assumptions, determine security decisions and minimize business risks.

The presented new risk classification allows managers to determine which risks can be managed using a rules-based model, and which require alternative approaches. We have investigated individual and organizational problems associated with conducting open, constructive discussions on risk management related to strategic choice, and we argue that companies need to take these discussions into account in the processes of developing and implementing their strategy.

Figure 2 illustrates the steps in the risk management framework.

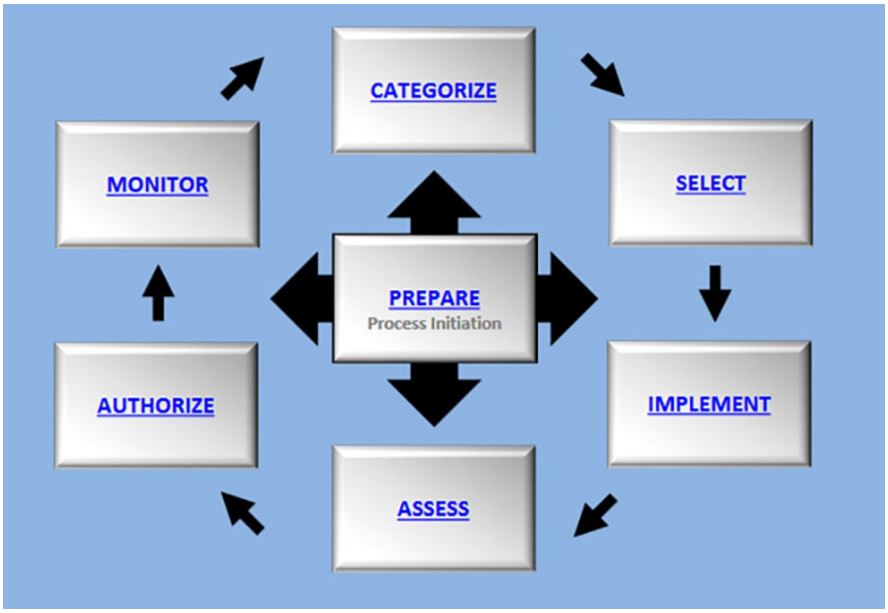

Fig. 2. Risk management framework.

The methodology begins with a thorough analysis of the selected methodologies and standards. This analysis serves as the basis for the subsequent steps in the process. It provides a comprehensive understanding of the strengths and weaknesses of each approach, enabling the development of a more effective risk assessment framework.

One of the most important aspects of this methodology is the consideration of the organization's existing assets. This step involves identifying the assets that need protection and understanding their vulnerabilities. This information is critical to making informed risk mitigation decisions.

To facilitate the collection and analysis of data, a large database is created to store both input and output parameters. This database serves as a repository of all relevant information, making it easily accessible during the assessment process.

The most important step is to compare the highlighted input and output data. Based on the analysis of these data, recommendations for risk accumulation and action are formulated.

This process ensures that each piece of information is effectively utilized to improve information security.

The development of recommendations for each highlighted parameter is a key element of this methodology. These recommendations are not arbitrary, but are based on expert judgment using the Delphi method. Competent experts in the field provide insights and experience directly relevant to the organization or firm being assessed.

To enhance the practicality of this approach, it provides functionalities for both clients and experts. In this way, the evaluation process incorporates the views of both parties, resulting in more comprehensive recommendations.

One of the features of this method is the creation of a software tool for analyzing, identifying and preventing information security risks. This software streamlines the assessment process, making it more efficient and accessible to organizations.

In addition, the methodology includes the calculation of convergence and gradation of data significance. This step allows prioritizing the identified risks and focusing resources on the most critical areas.

Finally, a key feature is the automated output of results for each parameter. This automated system categorizes risks into priority, medium and lower priority parameters. With the recommendations developed, organizations can make informed decisions to address each risk.

The final risk report should describe each threat, associated vulnerabilities, assets at risk, potential impact on IT infrastructure, likelihood of occurrence, and recommended controls and cost.

3 Conclusion

In conclusion, this comprehensive methodology for information security risk assessment and management is a significant step forward in ensuring the protection of critical data. By combining various methodologies and standards, expert assessments and automated tools, it provides a holistic approach to identifying, mitigating and addressing information security risks. In an era where data breaches and cyber threats are a constant challenge, implementing such a methodology can be a critical factor for organizations looking to strengthen their information security defenses.

The work was performed under Agreement No. 40469-21/2022-k dated 06/30/2022.

References

1. M.A. Maslova, Scientific result. Information technologies **7(4)**, 34-40 (2022)
2. M.A. Maslova, E.N. Tishchenko, *Problems of design, application and security of information systems in the digital economy,* proceedings of the XIX International Scientific and Practical Conference, 28-29 October 2019, Rostov-on-Don, 211-215 (2019)
3. I.N. Kartsan, Natural and Technical Sciences **6(181)**, 19-21 (2023)
4. V.S. Averyanov, I.N. Kartsan, Information protection. Insight **1(109)**, 18-23 (2023)
5. V.S. Averyanov, I.N. Kartsan, Voprosy kyberbezopasnosti **2(54)**, 65-72 (2023). https://www.doi.org/10.21681/2311-3456-2023-2-65-72
6. A.A. Kuznetsov, M.A. Maslova, Marine strategy and policy of Russia in the context of ensuring national security and sustainable development in the XXI century, **2**, 269-273 (2019)

7. M.A. Maslova, V.S. Averyanov, *Information security*, Collection of reports of the All-Russian School of Young Scientists, 14-18 November 2022, Novosibirsk, 40-46 (2022)
8. M.A. Maslova, E.N. Tishchenko, *Problems of design, application and security of information systems in the digital economy*, Proceedings of the XXI International Scientific and Practical Conference, 29-30 November 2021, Rostov-on-Don, 77-82 (2021)
9. I.N. Kartsan, E.A. Kontyleva, Modern Innovations, Systems and Technologies **3(2)**, 201-212 (2023). https://www.doi.org/10.47813/2782-2818-2023-3-2-0201-0212
10. V.A. Akselrod, V.S. Averyanov, I.N. Kartsan, In the collection: Russian science, innovation, education - ROSNIO-2022, 142-147 (2022). https://www.doi.org/10.47813/rosnio.2022.3.142-147
11. A.O. Zhukov, I.N. Kartsan, V.S. Averyanov, Information and Telecommunication Technologies **51**, 39-45 (2021)
12. I.N. Kartsan, A.O. Zhukov, Information and Telecommunication Technologies **52**, 19-26 (2021)