DOI: https://doi.org/10.53486/dri2024.19
UDC: 004.056:[005.5:005.334]

CYBERSECURITY AS A PART OF OPERATIONAL RISK MANAGEMENT

Olga CAMINSCHI, PhD student

ORCID number 0000-0003-0854-2237

Abstract: *In today's environment, operational risk management is a key component of organizational risk management. Given the potential impact of risks on business operations, effective management is an essential part of an organization's development strategy. With the rapid advancement of information technology and the digitalization of businesses, the need for robust cybersecurity systems is becoming increasingly apparent. Achieving a balance between adapting to the digital world and effectively managing cybersecurity is crucial for maintaining competitiveness and customer trust. Additionally, cyber threats can result in not only financial losses but also heightened reputational and compliance risks, as organizations must adhere to various regulatory requirements. It is also important to note that cyber risks are interconnected with business processes and infrastructure, integrating into the broader operational risk management framework.*

Key words: *operational risk, technologies, cybersecurity, digitalization, risk mitigation, business continuity.*

JEL: G32

1. Introduction

To enhance organizational competitiveness and adapt to modern business conditions, digitalization has become a key component of development strategies. However, as organizations increasingly rely on digital technologies, cybersecurity has emerged as a critical aspect of operational risk management. Ensuring compliance with cybersecurity standards not only mitigates potential threats but also optimizes business processes and safeguards profitability. Consequently, there has been a notable global increase in spending on cybersecurity technologies and services. Figure 1 illustrates the dynamics of technology spending, including cybersecurity investments, from 2017 to 2027 (forecast).

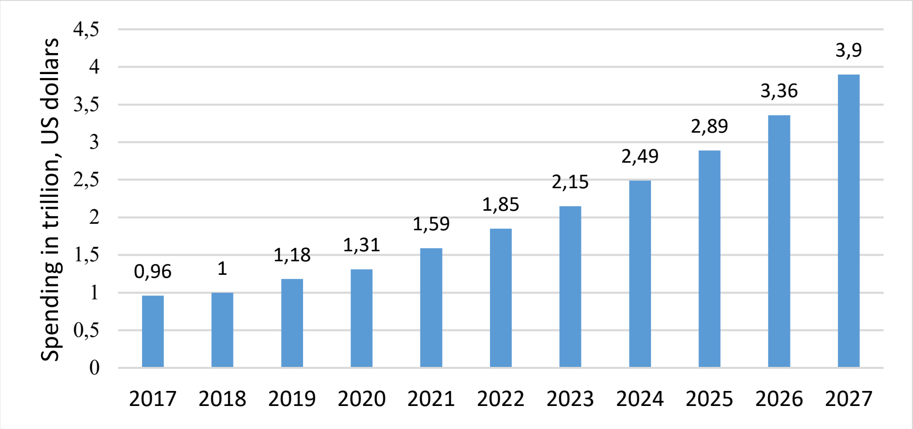

Figure 1. Spending on digital transformation technologies and services worldwide from 2017 to 2027

Source: https://www.statista.com/statistics/870924/worldwide-digital-transformation-market-size/

With the rapid development of information technology and the global integration of digital systems, managing operational risks has become increasingly complex, requiring a holistic approach. In today's organizations, cybersecurity is an essential component of operational risk management, demanding focused attention. It is crucial to recognize that cybersecurity threats, such as data breaches, system failures, and cyberattacks, can not only lead to financial losses but also disrupt business continuity and significantly heighten reputational risks, potentially resulting in a loss of customer trust.

While cyber risks were initially regarded as a specialized IT domain, they are now deeply integrated into all facets of operational activities, influencing business processes and the performance of products and services. Given this broad impact, a systematic approach to management is essential, as building a robust cybersecurity framework extends beyond technical issues and must be reflected in the organization's overall development strategy. Operational risk management must address the prevention of technical failures, protection of sensitive data, and ensuring the continuity of business processes—further emphasizing cybersecurity's pivotal role within the operational risk management system.

Operational risk is a type of risk that organizations face across all industries. According to the Basel Committee on Banking Supervision, operational risks are driven by the following risk factors:

- ✓ People;
- ✓ Systems;
- ✓ External events;
- ✓ Processes.

These factors encompass a wide range of potential threats, including IT system failures, fraud, industrial disasters, or human error. At the same time, with the advancement of digital transformation, operational risks are increasingly taking on a digital dimension. Today, conducting business is inherently linked to the use of information systems, the shift to electronic management systems, and the growth in the volume of data being processed. Consequently, attacks on these systems can result in operational disruptions or critical events with significant impact. This underscores the importance of building a robust cybersecurity framework as part of operational risk management.

The purpose of this article is to examine the relationship between cybersecurity and operational risk management and to explore contemporary approaches and tools that effectively counter cyber threats. This will involve identifying the main types of cyber risks, assessing their potential impact on organizational operations, and providing practical recommendations for strengthening information security systems in organizations.

2. Fundamentals of operational risk management

Since operational risks are related to a company's daily activities and arise from ineffective processes, human errors, or other factors, managing these risks is crucial for maintaining business resilience. Figure 2 illustrates the risk management process according to its stages.

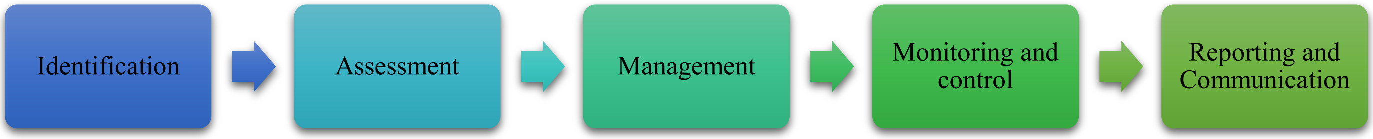

Figure 2. Stages of operational risk management

Source: Developed by the author

The first stage in managing operational risks is risk identification. This process involves identifying not only existing risks (which have materialized) but also potential threats that could affect the organization's activities. By developing a risk identification system, it is possible to detect potential threats in a timely manner and prepare strategies to mitigate them. The main tools used by organizations for risk identification are:

A) Risk and control self-assessment (RCSA). This method allows employees from various departments to assess risks and control measures directly. Involving staff who are directly involved in specific business processes ensures an assessment of each stage of the department's activities. By filling out various questionnaires or self-assessment reports, departments identify risks in their areas of responsibility.

B) Process mapping. This tool helps visualize the process by creating a business flow diagram or process flowchart. The methodology allows understanding at which stage of the analyzed process risks might arise or where the process can be improved.

C) Business impact analysis (BIA). To determine critical processes and resources, an assessment of the consequences for the business in the event of risk occurrence is conducted. Through filling out questionnaires, interviewing key staff, and analyzing business operations, the management body identifies critical processes for the organization. Subsequently, a continuity plan is developed to ensure the organization's operations in light of critical processes.

At the same time, a risk assessment matrix is often used to evaluate and manage operational risks directly. This method helps assess both the likelihood and potential impact of each risk and is commonly presented as a color-coded matrix (Figure 3).

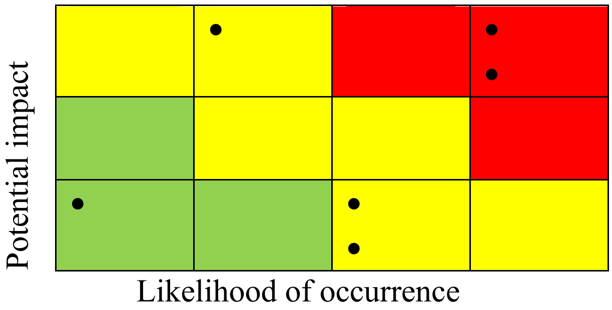

Figure 3. Visualization of risk categories

Source: developed by author

It is important to establish thresholds for each level based on the business process being examined and its significance to the organization, as well as the acceptable level of risk.

Additionally, *the FMEA (Failure Modes and Effects Analysis)* method is also used for risk analysis. The aim of this tool is to reduce the likelihood and impact of system failures through timely improvements. To achieve this, potential failure modes in a process or product are identified, and the consequences of each failure for the system are analyzed. Then, the causes contributing to the failure and its impact are determined to prioritize actions.

Thus, in managing operational risks, various aspects of the organization's activities and impact factors, including information technology, are assessed. This, in turn, confirms the integration of cybersecurity into operational risk management.

3. Methods for managing cyber threats in the context of operational risk management

To ensure the security and stability of businesses amidst the constant threat of cyberattacks, it is essential to develop an operational risk management system and advance technology. At the same time, cyber threats have become one of the most pressing issues for organizations globally, across various sectors. Figure 4 illustrates the distribution of cyberattacks by industry worldwide in 2023.

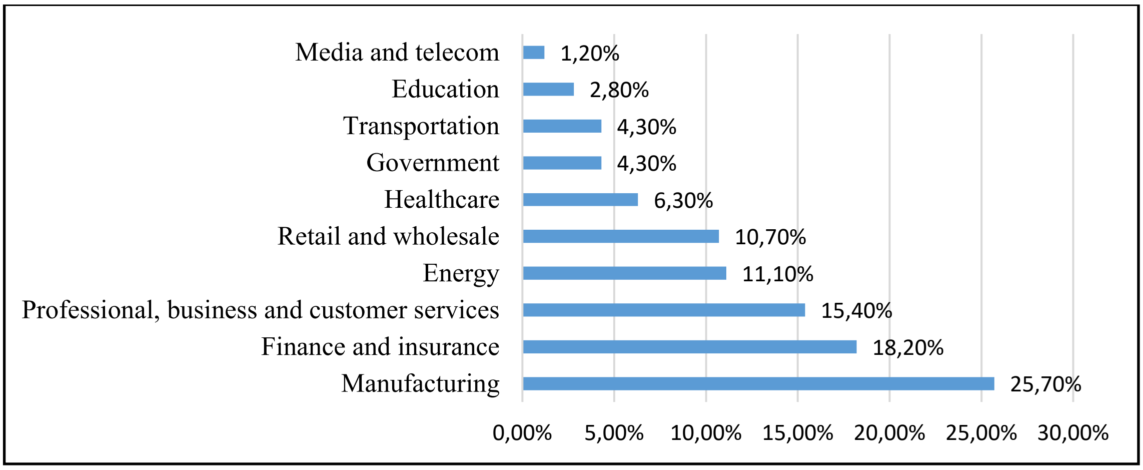

Figure 4. Distribution of cyberattacks across worldwide industries in 2023

Source: https://www.statista.com/statistics/1315805/cyber-attacks-top-industries-worldwide/

To understand how cybersecurity integrates into the operational risk management system, it is essential to analyze the main types of cyber threats.

Viruses and Worms Viruses are malicious programs that embed themselves in files and spread through email, data exchanges, and downloaded files. They can damage or destroy data and disrupt system operations. Worms, unlike viruses, are self-replicating malicious programs that spread through networks and do not require user interaction. They can slow down the network and overload the system. In the context of operational risk management, it's important to consider the potential impact of such threats on business processes and develop plans to minimize their consequences.

Spyware collects information about users without their knowledge and can transmit this data to malicious actors. It can lead to the leakage of confidential information such as passwords and credit card details. Managing such risk requires implementing monitoring and data protection mechanisms, as well as developing security policies to prevent leaks.

Ransomware encrypts data on an infected computer and demands a ransom for decryption. This can paralyze a company's operations and lead to significant financial losses. In the context of operational risk management, strategies should be developed for data backup and incident recovery plans.

Phishing is a form of social engineering where attackers spoof emails, messages, or websites to gain access to users' personal information. Effective management of this risk involves training employees to recognize phishing attacks and avoid falling victim to them.

Denial of Service (DoS/DDoS) attacks aim to overwhelm a system or network to take it down. This can disrupt access to crucial resources and services. As part of operational risk management, it is essential to implement protection against such attacks and develop plans for system recovery in case of an attack.

SQL Injection allows attackers to insert malicious SQL queries into a web form to gain unauthorized access to a database and retrieve or alter data. Managing this risk involves implementing web application protection methods and regular vulnerability testing.

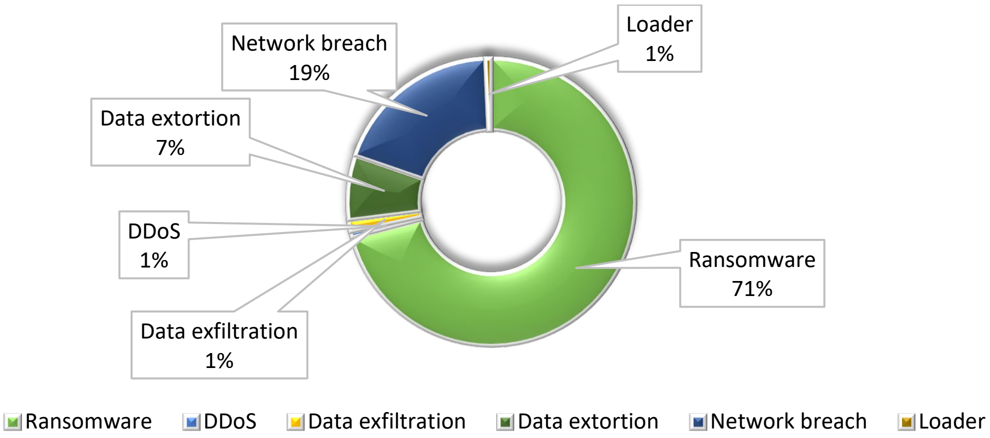

Figure 5. Distribution of detected cyberattacks worldwide in 2023, by type

Source: https://www.statista.com/statistics/1382266/cyber-attacks-worldwide-by-type/

Therefore, a wide range of cyber threats can potentially affect an organization's operations. To effectively manage cyber threats, it is essential to develop a comprehensive risk management process. This involves employing various methods and techniques. Regular updates to operating systems, applications, and antivirus software help close vulnerabilities that attackers might exploit. This is a key element of an operational risk management strategy aimed at preventing potential attacks. Also, antivirus software detects and removes malicious software, while firewalls help block unauthorized access to the network. These measures help minimize risks associated with cyberattacks and support overall system security.

It is important to highlight that people play a critical role in preventing cyber threats. Training employees in security basics, such as recognizing phishing emails and using passwords safely, helps prevent many attacks. This is also part of operational risk management, as humans are often the weakest link in security.

Data encryption protects information from unauthorized access, even if data falls into the hands of malicious actors. This is critical for managing operational risks associated with data breaches. Regular data backups enable information recovery in case of an attack, such as ransomware. This is part of an operational risk management strategy, ensuring the ability to quickly recover from incidents. Also, regular security checks, such as penetration testing and system audits, help identify and address vulnerabilities before they can be exploited by attackers. These actions contribute to managing operational risks by preventing potential incidents. Having a clear incident response plan allows for rapid and effective reaction to cyber incidents, minimizing damage and restoring normal system operations.

Cyber threats pose a serious risk in today's world, and managing them requires a comprehensive approach integrated with operational risk management. Understanding different types of threats and implementing effective protection methods will help safeguard data and systems from potential attacks and minimize risks. Regular updates, training, backups, and system checks are key components of a successful cybersecurity and operational risk management strategy.

4. Conclusions

In conclusion, integrating cybersecurity into operational risk management is a critically important aspect that cannot be ignored in the contemporary digital landscape. research has shown that cyber risks not only significantly increase the overall level of operational risks but also require a comprehensive approach for effective management. Effective management of cyber risks involves not only implementing advanced technologies and practices but also the active involvement of all organizational levels. Risk management strategies should include continuous updates to security policies, regular employee training, and proactive threat identification. It is recommended that organizations develop and implement comprehensive strategies that integrate best practices in cybersecurity and operational risk management. This will not only help minimize potential threats but also enhance the organization's overall resilience to changing external conditions.

Bibliographical references

1. Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.
2. Touhill, G. J. (2017). *Cybersecurity for executives: A practical guide*. Wiley.
3. Crouhy, M., Galai, D., & Mark, R. (2014). *The essentials of risk management*.
4. International Organization for Standardization. (2013). *ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements*.
5. Basel Committee on Banking Supervision. (2011). *Principles for the sound management of operational risk*.