The Assessment of Cyber Security's Significance in the Financial Sector of Lithuania

Julija Gavenaite-Sirvydiene* and Algita Miecinskiene

Department of Financial Engineering, Faculty of Business Management, Vilnius Gediminas Technical University, Sauletekio al. 11, 10223, Vilnius, Lithuania
E-mail: julija.gavenaite@gmail.com
**Corresponding Author*

Received 31 May 2022; Accepted 25 March 2023;
Publication 21 June 2023

Abstract

Constantly evolving high technologies provide new approaches to business development and deliver unknown business risks. Online financial services and operations are integral to everyday life, making cyber risk one of the most relevant risks for the financial sector's companies. As the survey conducted by the National Bank of Lithuania at the end of 2018 showed, the possibility of cyber threats and presumable effects on the financial system in Lithuania is one of the critical problems that should be prioritized. Therefore, it is essential to clarify what potential cyber threats in financial sector companies are considered the most significant and likely to occur. As well as identify how companies in the financial sector estimate their dispositions and preparedness for this cyber risk management and control. The findings of this research are significant for financial institutions as a tool to adopt their cyber risk management processes, increase preparedness and cyber security, and identify the possible threats to the organization.

Keywords: Cyber risk, cyber security, financial sector, risk management.

Journal of Cyber Security and Mobility, Vol. 12_4, 497–518.
doi: 10.13052/jcsm2245-1439.1243

1 Introduction

In recent years, the development of IT technologies, the Internet, and online services has completely changed the methods of communicating, working, and running the business, which became a crucial factor for economic growth worldwide. These changes created the opportunity for enterprises and private companies around the globe to benefit from the convenience, efficiency, and rapidity of online transactions, the interchange of data, and other information. Together it drastically increased the possibility of financial losses, data disclosure, and reputational issues caused by cyber-crimes (Stubley, 2013). Cyber security could be described as protecting all electronic devices and online storage (computers, mobile devices, servers, electronic systems, networks, online data, and cloud storage) from cyber-attacks (Advisen, 2018). In other words, it is electronic information security or security of information technology.

The cyber security issue was officially recognized worldwide in 2012 during the Global Economic Forum. That year, cyber security was named one of the five critical threats to humanity, ranking fourth on the scale of threats. Because of the constant increase of cyber-attacks worldwide every year and the financial and non-financial losses these attacks cause, the focus on creating methods and measures to identify, control, and prevent cyber risks is highly increased. Cyber-attacks constantly grow and are becoming more frequent. Hackers consistently improve their techniques, which usually happens much more rapidly than IT security evolves regarding cyber risks (Cebula, 2014).

Because of the variety of sensitive data, financial information, and resources, the financial sector faces growing pressure from cyber-attacks. Those risks came in very different forms and channels. The primary purpose of cyber security in the financial industry is to secure all the customer's data and assets. As online banking services become more developed, the possibility of cyber-attacks increases. (Chapelle, 2018). Because of these reasons, financial institutions need to implement cyber security programs, take all possible actions for cyber-attack prevention, and establish a plan for investments in cyber security.

The potential threat scope for financial institutions is being transformed continuously. The growth of online financial services, banking apps, and other mobile banking activities has significantly expanded the possible attack surface that hackers intend to exploit. Also, the geography of cybercrimes is transformed by global digitization processes. As billions of users in different

markets are involved in online activities, they could be considered new and easy targets to cybercriminals because of their low defense tools and lack of cybersecurity awareness. Financial institutions are forced to expand their ways to protect the financial system and networks as attackers become more targeted and intelligent. Because economic systems around the globe are becoming more connected and integrated, the defenders should pay attention to cooperation processes and create an integrated global environment for cyber security issues. Moreover, it is essential to involve small and medium size financial institutions in this process, especially in emerging markets; they are the most attractive target to cyber criminals.

The growing risk of cybercrime is also recognized by increasing investments in cyber defense tools. According to the KOVRR report, financial institutions have steadily increased their investments in cybersecurity. The investments are forecasted to reach $150 billion globally in 2022. Various factors could encourage increased attention and budget dedication to cyber security, for example, challenges in IT support growing awareness, and rising cyber-attack statistics. Research conducted by Deloitte (2020) proves a significant increase in investments in cyber security among financial institutions and that those institutions are already considering cybersecurity costs as part of permanent IT functions and budgets. This survey shows that in recent years institutions have been spending approximately 11% of their IT budget on cybersecurity tools. It is noted that this number is expected to be significantly growing in the future, considering the growth of cyber breaches. By choosing the right investment direction, financial institutions must understand the forces that affect and define the landscape of cyber threats. Understanding the significance of cyber threats and evaluating of most possible and harmful cyber attacks could guarantee the success and efficiency of potential investments that the company dedicates to cyber security.

The Object. Cyber security in the financial sector of Lithuania.

The Objectives. This article aims to evaluate the significance and relevance of cyber security in financial institutions, identify the most relevant cyber risks, and estimate preparedness levels in financial institutions.

Research methods. While preparing this research, these methods were used: qualitative and quantitative analyses of scientific literature and data, data comparison, multi-criteria decision analyses (TOPSIS method), and expert survey.

Motivation. Cyber security has become one of the most relevant risks to the financial sector, so it is crucial to put additional resources into understanding the possible threats and damage to the business. There are no practical tools or research proposals in the Lithuanian financial sector to help evaluate cyber security issues. Therefore this research can be a valuable tool for financial institutions to initiate cybersecurity activities in their company. Also, it is helpful to identify possible threats, evaluate their significance, and encourage to consider of additional measures or tools to provide secure financial services and a safe working environment.

2 Background and Related Work

Generally, cybersecurity protects all the systems connected to the Internet, for example, software, online data, and hardware, from cyber risks. Also, cyber security may be described as practices that help businesses and individuals avoid unauthorized access to private computers, databases, and other online information (Chang, 2012). In global connections and online activities, cyber security is mainly involved in every field – government, corporate finance, private households, and healthcare. All these organizations and individuals collect, store, process, use, and in other ways, operate with tremendous amounts of sensitive data on computers, networks, and other devices.

An effective cybersecurity process involves numerous layers of protecting tools across networks, computers, programs, or information. The methods, the people, and the tools must all accompany one alternative to generate a reliable defense before or after cyber-attacks (Sheth, 2021).

Acknowledgment of cyber security is essential, but it is also crucial to consider why it is significant. While hackers and attackers are implementing new technologies and developing their tools for cyber-attacks, organizations, and responsible employees should recognize the possible threats, why their company must maintain safety, and what measures should be used for protection and risk management (Assaf, 2008).

Regarding the research conducted by Bio-Team on cyber security's critical importance for financial institutions, securing the business environment in financial institutions will be one of the most relevant tasks in the future (2022). Financial institutions continue to be significant targets for cybercriminals. They hold sensitive personally identifiable information (PII) such as ID numbers, Social Security numbers, credit card information, and payment histories. Also, financial institutions are responsible for safeguarding these assets and ensuring this information's safe and legal usage. If the security

of personal information is not guaranteed, it can lead to a loss of customer data, trust and astonishing costs. Banks' total cost from a single data breach averages around $5.72 million per incident (Johnson, 2022).

It is essential for the organization to understand the possible methods that might be used against the sensitive data they possess. Depending on the industry and business type, various types of information and data are likely to be considered sensitive. However, the description of "sensitive information" should mainly involve anything expected to be under strict protection (General Data Protection Regulation, 2016). The table below shows five suggested examples of the recommended sensitive information.

Table 1 Types of sensitive information (compiled by the author, based on Wu (2015) and GDPR (2016))

Customer Information	Customer names, home addresses, payment card information, social security numbers, emails, application attributes, and any other information that allows identifying a person (directly or indirectly).
Employee Data	Employee data is comparable to customer information. Employees' names, addresses, social security numbers, banking information (for payment purposes), usernames, passwords used for company logins, or data associated with a credentialing process. This information is sensitive, making it critical for organizations to store it safely.
Intellectual Property & Trade Secrets	Nearly every company has proprietary information stored in their network, with a third party, or in a document management system. Intellectual property could be coded for software developers or schematics for hardware developers. This example of sensitive data could also extend to product specifications, competitive research, or anything that would fall under a non-disclosure agreement with a vendor.
Operational & Inventory Information	This example of sensitive data includes any generalized business operations or inventory figures. Businesses that sell physical products likely want sales figures to be kept private and accessed by their competitors. Sensitive data is not always personal or individual data but company-wide information that could impact business decisions, reputation, and operations if exposed.
Industry-Specific Data	Depending on the industry, specific examples of sensitive information may be needed to protect. The company's retail business operations must focus on protecting customers' payment data. In contrast, institutions in the healthcare sector must focus more on protecting digitally stored medical records and medical research data.

An essential part of financial institutions' data can be named as sensitive information, whether intellectual property, financial data, personal information, or other types of data for which unauthorized access or exposure could have negative consequences for the owner. Daily, organizations and companies transfer sensitive data and information to networks and different devices to provide services or do business; in these circumstances, cyber security becomes a discipline or method for information protection.

2.1 Global Review on Cyber Events

To properly understand the importance of cyber security, cyber-attacks' magnitude and the consequences of cyber crimes must be reviewed. International reinsurer Chubb has been tracking the key metrics of cyber crimes: actions causing cyber loss, the factor that caused cyber incidents (external or internal), and the number of related or impacted areas, as an essential part of the cyber claim handling process. These metrics are analyzed with general trend data and are valid for forecasting possible cyber events and losses, evaluating exposures, and reducing consequences (Chubb, 2020). As discovered earlier, cyber security in the financial sector is crucial for sustainable, secure, and successful business continuity. According to Chubb Cyber Index statistics, the global cyber incident rate is growing yearly (Figure 1).

This chart represents the percentage of the overall growth of cyber incidents by industry (financial sector) compared to the baseline year of 2012. As the figure shows, compared to 2012, overall, the percentage of cyber incidents evolved by 528%. In the financial sector globally, the increase reaches 104%. These statistics show that cyber incidents are becoming a significant issue globally to all industries and public sectors, not excluding financial institutions.

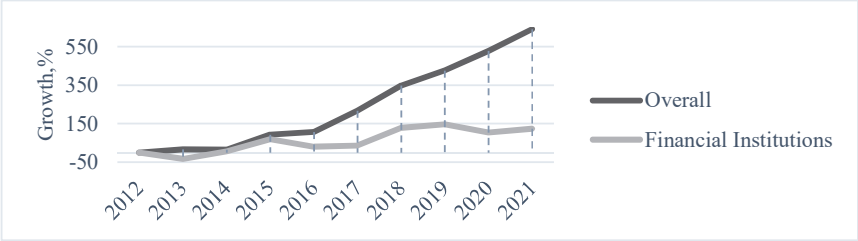

Figure 1 Global Incident Growth Compared to 2012.

Source: Chubb Cyber Incident Index Report.

Table 2 Actions causing cyber incidents. Source: Chubb Cyber Incident Index Report

Actions Causing Cyber Incidents	Share (%)
Unknown	32
Hacking	26
Social	14
Malware	12
Error	10
Misuse	3
Physical	3

Table 3 Source of actions causing cyber incidents. Source: Chubb Cyber Incident Index Report

Source of Actions Causing Cyber Incidents	Share (%)
External	56
Unknown	28
Internal	11
Partner	5

Moreover, it is essential to notify those actions causing cyber incidents that may arise from various sources and be targeted to a specific part or resource of the organization. According to Chubb Cyber Index, a few significant actions cause cyber incidents (Table 2).

Actions that are recognized as causing cyber incidents are: Malware (viruses, worms); Hacking (Distributed Denial of Service or DDoS attacks); Social (phishing, blackmail); Misuse (privacy violations); Physical (theft, tampering, snooping); Error (lost devices, misconfiguration, programming errors); or unknown. It can be affirmed that most actions are hardly recognized by the affected company and get into the unknown actions category. This phenomenon suggests that plenty of businesses still do not take cyber risk management actions and only state violations and cyber incidents after submission of a loss or harm. Also, 26% of activities that cause cyber incidents are hacking. Obtaining unauthorized or criminal access to or control of a computer system, server, or network is a hazardous risk for financial companies with massive amounts of sensitive data.

To better understand possible threats and prepare effective management protocol, it is essential to identify whether the source of cyber risk is internal or external. According to the Chubb Cyber Index review, more than half of cyber incidents are caused by external factors (Table 3).

This data represents a breakout of actions that contributed to or caused a cyber-incident and is categorized as External, Partner, Internal, or Unknown.

Table 4 Assets affected by cyber incidents. Source: Chubb Cyber Incident Index Report

Assets Affected by Cyber Incidents	Share (%)
Unknown	36
Servers/data	30
Network	14
User device	8
People	8
Media	3
Public Terminal	1

External actions mainly refer to someone an organization does not have a relationship with, including hackers. Partners are individuals or entities an organization has a business relationship with, including vendors or customers. Internal refers to employees and volunteers. Unknown applies to those instances where it is unknown who or what caused a cyber-incident. Each of these four categories may include actions with malicious intentions and actions without malicious intent.

Finally, while defining the significance of cyber security in the financial sector, it can be noted that very different parts of the organization may be affected and damaged (Table 4).

In the provided table above, assets refer to what was compromised during the cyber incident, such as a server, the network, a user device, a public terminal (a computer system that provides a service to the public or is for general use; for example, an ATM), media, or even people. Servers and data are the assets most likely to be affected or harmed by cyber-attacks.

According to the National Institute of Standards and Technology (NIST), global damages caused by cybercrime will cost more than $6 trillion by 2021. The damage cost estimation is based on historical cybercrime figures, including recent year-over-year growth and organized crime hacking activities, a cyber attack surface that will be greater in 2021 than five years ago. Cybercrime costs include: damage and destruction of data, stolen money, lost productivity, theft of intellectual property, robbery of personal and financial data, embezzlement, fraud, post-attack disruption to the ordinary course of business, forensic investigation, restoration, and deletion of hacked data and systems, and reputational harm.

In 2020, because of the Covid-19 global pandemic situation, cyber risks became even more relevant. The coronavirus outbreak has led to a massive number of employees who started working remotely. Employees should increase their awareness and knowledge of possible cyber incidents while working remotely to keep the working environment safe. Therefore, financial

institutions must effectively and actively organize training, self-education tools, and other measures to increase cyber security awareness. Cybersecurity Ventures (2021) estimate that cybercrime damage costs could double during the coronavirus outbreak. The most concerning issues are phishing scams, ransomware attacks, insecure remote access to corporate networks, remote workers exposing login credentials and confidential data to family members, and other threats.

As the volume and sophistication of cyber-attacks grow, companies and organizations, especially those tasked with safeguarding information relating to national security, health, or financial records, need to take steps to protect their sensitive business and personnel information.

3 Methods

When conducting research, various aspects of the possible and acceptable solutions are frequently considered – both in terms of potential costs and benefits to the organization. Multiple-Criteria Decision Analysis (MCDA) is used for selecting the solution which is the best in several respects considering the background circumstances. TOPSIS multi-criteria expert decision analyses method was chosen as the target of this paper to evaluate the significance of cyber security in the financial institutions of Lithuania.

A Multi-Criteria Analysis is a decision-aiding technique to analyze alternatives to complex problems. The analytical process is systematic, structured, open, and accountable (Opricovic, 2004). Multi-criteria decision analysis (MCDA) has been frequently used in management to evaluate decision-making options, which involve achieving multiple criteria. (Markovic, Z. 2010). This process also may be defined as an umbrella term to describe a collection of formal approaches which seek to take explicit account of multiple criteria in helping individuals or groups explore decisions that matter. (Belton, 2002)

The MCDA process has four key components:

1. A set of alternative options.
2. A set of criteria for comparing the alternatives.
3. Weighting to attach a measure of importance to each criterion.
4. A method of ranking the alternatives based on how well they satisfy the criteria.

Generally, the descriptions stated above summarize three different dimensions of the MCDA method. First, the formal approach of research. Secondly,

there are multiple criteria, and finally, that decision in the organization is made by individuals or groups. These three dimensions are why MCDA has been accepted as one of the most widely applied models in business management and the decision-making process. For further analyses, the TOPSIS method is chosen and will be used to evaluate the significance of cyber security in the financial sector of Lithuania.

3.1 TOPSIS Method Review

TOPSIS is a broadly accepted model proposed by Hwang and Yoon in 1981. The method is based on the concept that the chosen alternative should have the shortest geometric distance from the positive ideal solution and the longest geometric distance from the negative ideal solution. This method ranks alternatives based on the shortest distance from the positive ideal solution and the farthest distance from the negative ideal solution. TOPSIS is a verified tool for managing multi-criteria decision-making (MCDM) problems, and the powerful tool provides the capability to decide effectively.

The TOPSIS procedure consists of the following steps (Velasquez, 2013):

STEP 1: Establish a performance matrix. The decision matrix column contains column criteria (n) and is on the line as an alternative (m).

$$M = \begin{array}{c} \\ \\ A_1 \\ A_2 \\ \vdots \\ A_m \end{array} \begin{array}{c} \begin{array}{cccc} w_1 & w_2 & \cdots & w_n \\ C_1 & C_2 & \cdots & C_n \end{array} \\ \begin{pmatrix} z_{11} & z_{12} & \cdots & z_{1n} \\ z_{21} & z_{22} & \cdots & z_{2n} \\ \vdots & \vdots & \ldots & \vdots \\ z_{m1} & z_{m2} & \cdots & z_{mn} \end{pmatrix} \end{array} \tag{1}$$

STEP 2. Normalize the decision matrix. In the classical TOPSIS approach, the normalized performance matrix can be obtained using the following transformation formula:

$$n_{ij} = z_{ij} \Big/ \sqrt{\sum_{j=1}^{m} (z_{ij})^2}\,, \quad j = 1, \ldots, n,\ i = 1, \ldots, m. \tag{2}$$

Consequently, with this normalization, each attribute has the same unit scale. In [11, 24], it can be seen how the TOPSIS approach can implement different operating options in the step corresponding to the normalization.

STEP 3. Calculate the weighted normalized decision matrix. It is well known that the weights of criteria in decision-making problems have different means, and some have different importance. The weighted normalized value is calculated as follows:

$$v_{ij} = w_j n_{ij}, \quad i = 1, 2, \ldots, n; \quad j = 1, 2, \ldots, m. \tag{3}$$

These weights can be obtained differently: direct assignation, AHP, and others.

STEP 4. Determine the positive ideal and harmful ideal solutions. The positive ideal value set A^+ and the negative ideal value set A^- are determined as follows:

$$A^+ = \{v_1^+ \ldots v_n^+\} = \left\{ \left(\max_i v_{ij},\ j \in J \right) \left(\min_i v_{ij},\ j \in J' \right) \right\}$$
$$i = 1, 2, \ldots, m$$
$$A^- = \{v_1^- \ldots v_n^-\} = \left\{ \left(\min_i v_{ij},\ j \in J \right) \left(\max_i v_{ij},\ j \in J' \right) \right\}$$
$$i = 1, 2, \ldots, m \tag{4}$$

Where J is associated with benefit criteria, and J′ is associated with cost criteria.

STEP 5. Calculate the separation measures. The separation of each alternative from the positive ideal solution (PIS)A+ is given as follows.

$$d_i^+ = \left\{ \sum_{j=1}^{n} (v_{ij} - v_j^+)^2 \right\}^{\frac{1}{2}}, \quad i = 1, \ldots, m \tag{5}$$

Moreover, the separation of each alternative from the negative ideal solution (NIS)A-is as follows.

$$d_i^- = \left\{ \sum_{j=1}^{n} (v_{ij} - v_j^-)^2 \right\}^{\frac{1}{2}}, \quad i = 1, \ldots, m \tag{6}$$

In this case, we use them-multi dimensional Euclidean distance.

STEP 6. Calculate the relative closeness to the ideal solution. The relative closeness Ri to the ideal solution can be expressed as follows:

$$R_i = \frac{d_i^-}{d_i^+ + d_i^-}, \quad i = 1, \ldots, m \tag{7}$$
$$\text{If } \bar{R}_i = 1 \rightarrow A_i = \bar{A}^+$$
$$\text{If } \bar{R}_i = 0 \rightarrow A_i = \bar{A}^-$$

Where the Ri $= 1$ value lies between 0 and 1, the closer the $\bar{\text{R}}$i $= 1$ value is to 1, the higher the priority of the h alternative.

STEP 7. Rank the preference order. Rank the best alternatives according to Ri in descending order.

To sum up, this TOPSIS method has advantages such as the ability to recognize the proper alternative immediately, it is usable for situations with many alternatives and attributes, and it is based on an aggregating function representing "closeness to the ideal. Besides the advantages, there are drawbacks like lack of provision to weight elicitation and check the consistency of judgments. Also, this method needs to consider the relative importance of distances.

3.2 Provisions for Experts' Interviews

Using the multi-criteria expert decision analyses method (TOPSIS), the significance of cyber security in the financial sector companies was evaluated. To conduct valuable and reliable data, these requirements for the experts were established:

1. Represents a financial institution (either bank or insurance company);
2. Has at least ten years of experience in finance;
3. Takes a head position in one of these areas: IT security, data protection, or risk management.

The respondents were selected from six organizations – banks and non-life insurance companies operating in Lithuania. The questionnaire for experts involved these general issues in measuring:

Table 5 Questionnaire for experts' evaluations

Criteria	Alternatives	Significance Evaluation
The most critical cyber security area in the organization	Data security Network security Mobile security Database and infrastructure security End-user education Cloud Security Disaster recovery and business continuity	Rating range from 0 to 1. A total sum of all criteria – 1.
The most harmful type of cyber-attack	Phishing Account takeover and credential abuse attacks Malware (viruses, worms, Trojans) Web application attacks Insider threats Ransomware Denial of service (DoS/DDoS) attacks	
The type of cyber-attack that is most likely to occur in the organization	Phishing Malware Ransomware Web application attacks Account takeover and credential abuse attacks Insider threats Denial of service	
Organization's preparedness for cyber events	Malware Insider threats Account takeover and credential abuse attacks Phishing Web application attacks Ransomware Denial of service	
Cyber-attacks importance and relevance in the context of other existing financial and operational risks for their business	Financial risk (liquidity, credit, tax) Cyber Risk Market Risk (equity, interest rate, currency) Operational risk (sales, marketing, people) Compliance Risk (regulatory, legal) Strategic risk (communication, investing, resource)	

4 Research Results

After completing interviews with experts and collecting their evaluations, the steps to process the data were taken according to the TOPSIS method. After processing data and ranking values in descending order, the final evaluations were completed.

Firstly, the importance of different cybersecurity areas was evaluated (Table 6); the following results were conducted:

According to experts' evaluation, data security was selected as the most significant field of cyber security in financial organizations. Network security was selected as the second most important field of cyber security. Also, it is essential to note that mobile security was pointed out as the third cyber security field of importance in financial institutions. This issue is even more relevant since the global pandemic transferred most financial services and transactions to the online environment.

Further, in the survey, the experts rated the common types of cyberattacks from the most significant and harmful to the company's financial stability to the least relevant (Table 7).

Table 6 The most critical cyber security area in the organization. Source: concluded by authors

Alternatives	Total Score	Rank
Data security	1	1
Network security	0.7305766	2
Mobile security	0.7156353	3
Database and infrastructure security	0.4745102	4
End-user education	0.3090169	5
Cloud Security	0.2421017	6
Disaster recovery and business continuity planning	0.0921756	7

Table 7 The most harmful type of cyber-attack. Source: concluded by authors

Alternative	Total Score	Rank
Phishing	0.85881215	1
Account takeover and credential abuse attacks	0.82834172	2
Malware	0.71563534	3
Web application attacks	0.37330926	4
Insider threats	0.33996830	5
Ransomware	0.30901699	6
Denial of service	0.06528343	7

Table 8 The type of cyber-attack that is most likely to occur in the organization. Source: concluded by authors

Alternative	Total Score	Rank
Phishing	0.90782439	1
Malware	0.82834172	2
Ransomware	0.60069950	3
Web application attacks	0.45416345	4
Account takeover and credential abuse attacks	0.30157246	5
Insider threats	0.24210172	6
Denial of service	0.21712927	7

As the experts indicate – the most harmful cyber-attack is phishing – the emails that appear to be from trusted sources (the bank or insurance company the client uses) to gain sensitive information. The second type of cyber-attack the experts selected is account takeover and credentials abuse attacks. These attacks are significant for financial institutions because they possess sensitive customer data.

Further in the research, the experts evaluated the likelihood of cyber-attack occurrence in the organization's activity type and implemented cyber risk management measures, and other measures to prevent cyber incidents (Table 8).

According to experts ' opinion, the results here closely correlate with the question above and indicate that the possible risks in the financial institution are phishing and malware. This indication approves the significance of account or personal credentials safety issues.

The company's preparedness to identify and resolve the cyber-attack is an integral part of the cyber security environment in the company. According to the expert's evaluations, financial institutions in Lithuania are prepared to manage malware, insider threats, and account takeover/credential attacks. (Table 9).

According to experts, financial institutions are the least prepared for ransomware and denial of service attacks.

Finally, the experts evaluated the importance of cyber security and cyber risks and ranked them as the second most important type of risk (Table 10).

Comparing cyber risks to other financial and operational risks occurring in financial institutions, the significance of cyber security is increasing. With financial and market risks, cyber risk concludes the most critical issue and part of business management that financial institutions focus on.

Table 9 Organization's preparedness for cyber events. Source: concluded by authors

Alternative	Total Score	Rank
Malware	0.70471480	1
Insider threats	0.68416134	2
Account takeover and credential abuse attacks	0.67787833	3
Phishing	0.61819561	4
Web application attacks	0.45682327	5
Ransomware	0.21712927	6
Denial of service	0.09217560	7

Table 10 Cyber risks' importance and relevance in the context of other financial and operational risks. Source: concluded by authors

Alternative	Total Score	Rank
Financial risk (liquidity, credit, tax)	0.68857860	1
Cyber Risk (malware, phishing, web attacks, account, or information takeover)	0.67095431	2
Market Risk (equity, interest rate, currency, commodity risks)	0.64611063	3
Operational risk (sales, marketing, people)	0.39331346	4
Compliance Risk (regulatory, legal)	0.32037724	5
Strategic risk (communication, investing, resource allocation)	0.26841742	6

5 Discussion

After analyzing the research results, it can be indicated that data security is considered the highest priority risk. It involves not only commercial information or financial data but also customers' sensitive and private information. This specific structure of owned data determines the high level of risk and consequences to the financial institution in case of a data security breach. Recently concluded research (Johnson, 2022) in financial institutions also confirms that the importance and priority of data security will significantly increase in the future. Financial institutions are constantly increasing their budgets and internal protocols for personal development and knowledge to prevent sensitive data breaches. Also, network and mobile security are highly important in the relevance to sensitive data protection which is one of the critical parts of business continuity elements.

Discussing the most significant and harmful cyber risk to the company's financial stability is phishing. As Most likely, the attackers aim to appropriate the financial credentials such as bank account details or passwords. The attack mostly comes from an external source aiming at data or networks, which fully complies with the nature of phishing attacks (Chubb, 2022). Currently,

financial institutions in Lithuania are facing increasing attacks and allocating more financial and management resources to protect their customers from phishing attacks. Phishing attacks in financial organizations may be harmful in a few different ways. For example, they may lead to internal databases or application credentials leakage and can be used as a link to extract sensitive company information or internal data. Under current circumstances of remote working and online usage of financial services, the obligation to ensure safe and fluent processes is becoming one of the top priorities for financial institutions. Moreover, Sheth (2021) also claims that in their research, it is important to identify different layers of tools that are dedicated to protecting networks and information. The attention should be focused especially on the human factor because training and knowledge of employees are the key factors leading to a secure work environment.

Discussing the company's preparedness to identify and resolve the cyber-attack, it can be noted, that in the Lithuanian financial sector companies already have identified their vulnerabilities and security gaps and put sighinifact attention to developing business resilience and preparedness level in case of phishing or account take over risk occurs. As the KOVRR report proved (2022), financial institutions are constantly increasing the amount of their investment in cybersecurity issues. The investments are predicted to reach 150 billion globally in 2023. According to the EU Cyber Security regulation, Lithuania will invest 1,6 billion EUR into developing cyber security until 2027. Continuous investments in the internal infrastructure, employee training, and consistent experience in identifying and solving those threats. As the attackers and their techniques evolve quickly, preparing an effective risk management model and fluently implementing it in the organization is challenging.

6 Conclusions and Future Work

Cybersecurity has become one of the top priority issues for financial institutions in recent years. Exceptionally, under pandemic situations – the safety of online data, storage, and information, together with adequately functioning online services and remote working environment, is considered a crucial issue to discover and manage.

Multi-criteria expert decision analyses method TOPSIS was selected as a suitable method to complete the research and evaluate the opinions of experts representing financial institutions such as banks and non-life insurance companies in Lithuania.

As the research results implicate, cyber risks are the second most significant risks to handle in a typical business risk environment. Based on the expert's indications, data security is the most significant field of cyber security for financial organizations because it covers specific commercial information, financial data, and sensitive and private information of customers. Phishing is the most harmful to a company's financial stability and is predicted as most likely to occur in the organization. Therefore, financial institutions must allocate a proper focus, including financial investments and human resources, to improve risk management systems and ensure business safety and continuity.

The risks that are most likely to occur in a financial institution are phishing and malware. This implication confirms the significance of account or personal credentials safely issued. In the context of the pandemic situation around the globe, changing working habits, and usage of financial services online, the necessity to provide safe and fluent processes is one of the top priorities for financial institutions.

Financial institutions specify that they are well prepared to manage and control malware and insider threats as they have experience and are implementing risk management policies. However, most relevant cyber risks, such as phishing or account takeover, are still in the process of creating proper control plans and tools.

The findings of this research play important implications for better understanding possible cyber security threats and vulnerable touchpoints in the organization. Based on these findings, it could be recommended for a financial institution's responsible staff to pay attention, prepare relevant tools for cyber risk management, and ensure the business environment and customer services are under effective security measures.

The limitation of this research is the lack of connectivity between specific cyber risks and possible damage to the financial institution. Therefore, future research could evaluate the financial impact of different cyber threats. For instance, regarding the type of institution (bank, insurance company, credit union), the most significant and likely to occur cyber threats are different. Therefore, they have a different financial impact and may cause higher or lower damage or reputational harm. Continuing to analyze cybersecurity issues in financial institutions, different types of cybersecurity tools could be investigated. For example, assessing the most effective and efficient cyber risk management tools regarding the type of organization.

References

Advisen. (2018). The Future of cyber risk modeling. 18 April, 2018, London. Available at: https://www.advisenltd.com/2018/04/24/the-future-of-cyber-risk-modeling/.

Assaf A, (2008). Automation, Stock Market Volatility, and Risk-Return Relationship. Investment Management and Financial Innovations, 3/2005.

Belton, V.; Stewart, T. Multiple Criteria Decision Analysis: An Integrated Approach. ISBN: 978-0-7923-7505-0.

Cebula, J.J.; L.R. Young. 2010. A taxonomy of Operational Cyber Security Risks. Technical Note CMU/SEI-2010-TN-028, Software Engineering Institute, Carnegie Mellon University.

Chang, A., Zhong, L., Grabosky, P., Citizen co-production of cyber security: Self-help, vigilantes, and cybercrime. Regulation & Governance (2018) 12, 101–114. DOI: 10.1111/rego.12125.

Chapelle, A., Crama, Y., Huebner, G., Peters, J.-P. 2018. Practical methods for measuring and managing operational risk in the financial sector: a clinical study. Banking & Finance 32(6).

Chubb Cyber Index: Providing Data-Driven Insight on Cyber Threat Trends. Available at: https://chubbcyberindex.com/#/incident-growth.

Cybersecurity Ventures Marcadet T. 2020. Navigating through Cyber Risk.

European Union (2016) Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC (GDPR).

Hwang, C.L. and Yoon, K. (1981) Multiple Attribute Decision Making: Methods and Applications. Springer-Verlag, New York.

Kaspersky Lab, "Damage Control: The Cost of Security Breaches," 2015. As of 4 January, 2018: https://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf.

KOVRR. Cybersecurity Investments vs. Actual Risk and Cyber Risk Mitigation. 2022. https://www.kovrr.com/blog-post/cybersecurity-investments-vs-actual-risk-and-cyber-risk-mitigation.

Markovic, Z. Modification of TOPSIS method for solving multi-criteria tasks. Yugoslav Journal of Operations Research 20(1). DOI: 10.2298/YJOR1001117M.

Merriam-Webster Inc./ Online Dictionary. Available at: https://www.merriam-webster.com/dictionary/cybersecurity.

National Bank of Lithuania. 2018. Survey: Cybercrimes are the most significant risk to the domestic financial system. Available at: https://www.lb.lt/en/news/survey-cybercrimes-are-the-greatest-risk-to-the-domestic-financial-system.

National Institute of Standards and Technology, Standards for Security Categorization of Federal Information and Information Systems, FIPS 199, 2004. As of 4 January 2018: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf.

Opricovic, S.; Tzeng, G-H. 2004. Compromise solution by MCDM methods: A comparative analyses of VIKON and TOPSIS. European Journal of Operational Research. 156:445–455.

Sheth, A.; Bhosale, S.; Kurupka, F. 2021. Research Paper on Cyber Security. Contemporary Research in India (ISSN 2231-2137. Special Issue: April 2021.

Stubley D. (2013). What is Cyber Security? Independent Information Security Center. Oxford.

Velasquez, M., & Hester, P. T. (2013). An analysis of multi-criteria decision-making methods. International Journal of Operations Research, 10(2), 56–66.

World Economic Forum. The Global Risks Report 2020. 15th edition, in partnership with Marsh & McLennan and Zurich Insurance Group. Available at: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf.

Wu, W.; Kang, R.; Li, Z. Risk assessment method for the cyber security of cyber-physical systems. In Proceedings of the 2015 First International Conference on Reliability Systems Engineering (ICRSE), Beijing, China, 21–23 October 2015.

Zhao, X.; Xue, L.; Whinston, A. 2009. Managing Interdependent Information Security Risks: An Investigation of Commercial Cyber insurance and Risk Pooling Arrangement Thirtieth International Conference on Information Systems, p. 189–239.

Biographies

Julija Gavenaite-Sirvydiene received a bachelor's degree in financial economics and a master's degree in business management. Currently a doctoral student at Vilnius Gediminas Technical University, in the economic engineering field. Generally, her research area includes insurance and reinsurance analyses, financial risks, and cyber security. The subject of a doctoral thesis is cyber security in the financial sector. The scientific activity that she has been participating in involves lecturing the financial risk management subject for bachelor students, participating in international conferences, and serving as an organizer of international scientific conferences. She is a member of Lithuania's Young Researches Society and used to serve as a board member of this organization.

Algita Miecinskiene received a bachelor's degree in civil engineering, a master's degree in business, and philosophy of doctorate in economics from Vilnius Gediminas Technical University (VILNIUS TECH). She has been working as an Associate Professor at the Department of Financial Engineering since 2004 and as a head of the Financial engineering department since 2016, Faculty of Business Management, VILNIUS TECH. Her research areas include risk management, effective pricing, personal finance,

and investments. She presents papers at conferences and is the author of more than 40 scientific publications and the author (co-author) of two textbooks. She has experience participating in international research, study projects, and international lecturing. She has been serving as a reviewer for highly respected journals.