VILNIUS GEDIMINAS TECHNICAL UNIVERSITY

Julija GAVĖNAITĖ-SIRVYDIENĖ

DEVELOPMENT OF CYBER SECURITY ASSESSMENT TOOL FOR FINANCIAL INSTITUTIONS

DOCTORAL DISSERTATION

SOCIAL SCIENCES,
ECONOMICS (S 004)

Vilnius, 2024

The doctoral dissertation was prepared at Vilnius Gediminas Technical University in 2019–2024.

Supervisor

Assoc. Prof. Dr Algita MIEČINSKIENĖ (Vilnius Gediminas Technical University, Economics – S 004).

The Dissertation Defence Council of the Scientific Field of Economics of Vilnius Gediminas Technical University:

Chairperson:

Prof. Dr Rima TAMOŠIŪNIENĖ (Vilnius Gediminas Technical University, Economics – S 004).

Members:

Assoc. Prof. Dr Raimonda MARTINKUTĖ-KAULIENĖ (Vilnius Gediminas Technical University, Economics – S 004),
Prof. Dr Javier OLIVER MUNCHARAZ (Polytechnic University of Valencia, Spain, Economics – S 004),
Prof. Dr Vaida PILINKIENĖ (Kaunas University of Technology, Economics – S 004),
Assoc. Prof. Dr Viktorija SKVARCIANY (Vilnius Gediminas Technical University, Economics – S 004).

The dissertation will be defended at the public meeting of the Dissertation Defence Council of the Scientific Field of Economics in the SRA-I Hall of Vilnius Gediminas Technical University at **9 a.m. on 31 May 2024.**

Address: Saulėtekio al. 11, LT-10223 Vilnius, Lithuania.
Tel.: +370 5 274 4956; fax +370 5 270 0112; e-mail: doktor@vilniustech.lt

A notification on the intended defence of the dissertation was sent on 30 April 2024. A copy of the doctoral dissertation is available for review at the Vilnius Gediminas Technical University repository https://etalpykla.vilniustech.lt, at the Library of Vilnius Gediminas Technical University (Saulėtekio al. 14, LT-10223 Vilnius, Lithuania) and the library of Lithuanian Center for Social Sciences (A. Goštauto str. 9, LT-01108 Vilnius, Lithuania).

Vilnius Gediminas Technical University book No 2024-023-M

https://doi.org/10.20334/2024-023-M

julija.gavenaite-sirvydiene@vilniustech.lt

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

Julija GAVĖNAITĖ-SIRVYDIENĖ

KIBERNETINIO SAUGUMO VERTINIMO PRIEMONĖS SUKŪRIMAS FINANSŲ INSTITUCIJOMS

DAKTARO DISERTACIJA

SOCIALINIAI MOKSLAI,
EKONOMIKA (S 004)

Vilnius, 2024

Disertacija rengta 2019–2024 metais Vilniaus Gedimino technikos universitete.

Vadovas

doc. dr. Algita MIEČINSKIENĖ (Vilniaus Gedimino technikos universitetas, Ekonomika – S 004).

Vilniaus Gedimino technikos universiteto Ekonomikos mokslo krypties disertacijos gynimo taryba:

Pirmininkas:

prof. dr. Rima TAMOŠIŪNIENĖ (Vilniaus Gedimino technikos universitetas, Ekonomika – S 004).

Nariai:

doc. dr. Raimonda MARTINKUTĖ-KAULIENĖ (Vilniaus Gedimino technikos universitetas, Ekonomika – S 004),
prof. dr. Javier OLIVER MUNCHARAZ (Valensijos politechnikos universitetas, Ispanija, Ekonomika – S 004),
prof. dr. Vaida PILINKIENĖ (Kauno technologijos universitetas, Ekonomika – S 004),
doc. dr. Viktorija SKVARCIANY (Vilniaus Gedimino technikos universitetas, Ekonomika – S 004).

Disertacija bus ginama viešame Ekonomikos mokslo krypties disertacijos gynimo tarybos posėdyje **2024 m. gegužės 31 d. 9 val.** Vilniaus Gedimino technikos universiteto SRA-I posėdžių salėje.

Adresas: Saulėtekio al. 11, LT-10223 Vilnius, Lietuva.
Tel.: (8 5) 274 4956; faksas (8 5) 270 0112; el. paštas doktor@vilniustech.lt

Pranešimai apie numatomą ginti disertaciją išsiųsti 2024 m. balandžio 30 d.

Disertaciją galima peržiūrėti Vilniaus Gedimino technikos universiteto talpykloje https://etalpykla.vilniustech.lt ir Vilniaus Gedimino technikos universiteto bibliotekoje (Saulėtekio al. 14, LT-10223 Vilnius, Lietuva), ir Lietuvos socialinių mokslų centro bibliotekoje (A. Goštauto g. 9, LT-01108 Vilnius, Lietuva).

Abstract

Cyber security is becoming one of the most critical issues for companies willing to empower their growth and business success by using online technologies. The development of online services has completely changed the ways and processes of financial services. The scientific problem formulated in the dissertation is the necessity to properly evaluate cyber security levels in financial institutions arising due to various sector-specific vulnerabilities. The dissertation's research object is the assessment of cyber security in a financial institution.

The goal of this dissertation is to create a comprehensive tool that would allow financial institutions to evaluate the cyber security level individually within the organisation. The following main tasks are resolved within the dissertation: (1) to investigate cyber risks and cyber-security features and importance, identify the main areas of cyber security with indicators representing each area's most significant features, based on scientific literature analyses, (2) to establish a methodology for a tool that allows the cyber security assessment in a financial institution, (3) to develop a unique questionnaire matrix to conduct an internal assessment of a financial institution's cyber security level based on the provided cyber security indicators, (4) to create a tool for the cyber security evaluation in financial institutions by proposing a composite cyber security index as a final result, (5) to assess cyber security in selected financial institutions to practically verify the proposed composite cyber security index.

The dissertation consists of the following parts: (1) a scientific literature analysis on cyber risks and cyber security, general features, legal requirements, and cyber risk assessment presumptions. This part of the research is a significant theoretical background for the following steps. (2) A methodology for creating a composite cyber security index. (3) Final development of a composite cyber security index that consists of these main parts: 4 major areas of cyber security; 22 specific indicators within the areas; specific weight for each indicator; model of questionaries for individual evaluation of each indicator within the organisation. The proposed tool for evaluating cyber security in financial institutions – the composite cyber security index – is considered a comprehensive and effective method to assess cyber security levels, indicate weaknesses and vulnerabilities, and initiate adjustments and improvements in the organisation.

Reziumė

Kibernetinis saugumas tampa vienu iš svarbiausių iššūkių įmonėms, siekiančioms padidinti savo augimą ir verslo sėkmę naudojant informacines technologijas. Internetinių paslaugų plėtra visiškai pakeitė finansinių paslaugų teikimo būdus ir procesus. Disertacijoje suformuluota mokslinė problema – būtinybė įvertinti kibernetinio saugumo lygį finansų institucijose, kadangi būtent šių institucijų veiklos specifika nulemia jų ypatingą pažeidžiamumą kibernetinėje erdvėje. Disertacijos tyrimo objektas – kibernetinio saugumo vertinimas finansų institucijose.

Disertacijos tikslas – sukurti įrankį, kuris leistų finansų institucijoms individualiai įvertinti savo kibernetinio saugumo lygį. Disertacijoje sprendžiami šie pagrindiniai uždaviniai: 1) išanalizuoti kibernetinės rizikos ir kibernetinio saugumo ypatumus bei svarbą ir nustatyti pagrindines kibernetinio saugumo sritis ir rodiklius, atspindinčius svarbiausius kiekvienos srities bruožus teoriniu aspektu, 2) sukurti metodiką priemonei, leidžiančiai įvertinti finansų institucijos kibernetinį saugumą, 3) sudaryti unikalų klausimyną, skirtą vidiniam kibernetinio saugumo lygio įvertinimui finansų institucijoje atlikti, remiantis pateiktais kibernetinio saugumo rodikliais, 4) sukurti finansų institucijų kibernetinio saugumo vertinimo priemonę, kaip galutinį rezultatą pasiūlant sudėtinį kibernetinio saugumo indeksą, 5) įvertinti kibernetinio saugumo lygį pasirinktose finansų institucijose ir taip praktiškai patikrinti siūlomą sudėtinį kibernetinio saugumo indeksą.

Disertaciją sudaro šios dalys: 1) mokslinės literatūros apie kibernetinio saugumo sampratą, bendruosius bruožus, teisinius reikalavimus ir kibernetinio saugumo vertinimo prielaidas analizė (ši tyrimo dalis yra reikšmingas teorinis pagrindas tolesniems tyrimo etapams); 2) sudėtinio kibernetinio saugumo indekso sudarymo metodika; 3) sukurtas sudėtinio kibernetinio saugumo indeksas, kurį sudaro šios pagrindinės dalys: 4 pagrindinės kibernetinio saugumo sritys, 22 konkretūs rodikliai pagal sritis, konkretus kiekvieno rodiklio svoris, klausimynų, skirtų vidiniam kiekvieno rodiklio vertinimui organizacijoje, modelis. Siūlomas finansų institucijų kibernetinio saugumo vertinimo būdas – *sudėtinis kibernetinio saugumo indeksas* – yra išsamus ir veiksmingas įrankis, leidžiantis įvertinti kibernetinio saugumo lygį, nustatyti silpnąsias vietas, inicijuoti pokyčius organizacijoje siekiant pagerinti kibernetinio saugumo lygį.

Notations

Abbreviations

AI – Artificial Intelligence (liet. *dirbtinis intelektas*);

CISA – Cyber Security and Infrastructure Security Agency (liet. *Kibernetinio saugumo ir infrastruktūros saugumo agentūra*);

CMMC – Cyber security Maturity Model Certification (liet. *kibernetinio saugumo brandos modelio sertifikavimas*);

CPS – The Crown Prosecution Service (liet. *Karališkoji prokuratūra*);

CSIRT – National or Governmental Cyber Security Incident Response Teams (liet. *nacionalinės arba vyriausybinės reagavimo į kibernetinio saugumo incidentus grupės*);

DoS – Denial of Services (liet. *paslaugos trikdymo ataka*);

EBA – European Banking Authority (liet. *Europos bankininkystės institucija*);

ECB – European Central Bank (liet. *Europos Centrinis bankas*);

EDF – The European Defence Fund (liet. *Europos gynybos fondas*);

ENISA – European Union Agency for Cyber Security (liet. *Europos Sąjungos kibernetinio saugumo agentūra*);

EU – European Union (liet. *Europos Sąjunga*);

GDPR – General Data Protection Regulation (liet. *Bendrasis duomenų apsaugos reglamentas*);

ICT – Information and Communication Technology (liet. *informacinės ir ryšių technologijos*);

IoT – Internet of Things (liet. *daiktų internetas*);

ISMS – Information Security Management System (liet. *informacijos saugumo valdymo sistema*);

IT – Information Technology (liet. *informacinės technologijos*);

NCSC – National Cyber Security Center (liet. *Nacionalinis kibernetinio saugumo centras*);

NIST – National Institute of Standards and Technology (liet. *Nacionalinis standartų ir technologijos institutas*);

NPV – Net Present Value (liet. *grynoji dabartinė vertė*);

OECD – Organisation for Economic Co-operation and Development (liet. *Ekonominio bendradarbiavimo ir plėtros organizacija*);

ROI – Return on Investment (liet. *investicijų grąža*);

SAW – Simple Additive Weighting Method (liet. *paprastasis adityvus svorių metodas*);

SSM – Single Supervisory Mechanism (liet. *bendrasis priežiūros mechanizmas*);

TOPSIS – Technique for Order of Preference by Similarity to Ideal Solution (liet. *artumo idealiajam taškui metodas*);

WFH – Working from Home (liet. *darbas iš namų*).

Content

Introduction

Problem Formulation

Cyber-attacks are becoming more frequent and sophisticated every year. Their costs are difficult to calculate, and losses vary across business sectors. Companies in the financial industry are one of the main targets of cyber-attacks due to the specific activities and sensitive data they use in their business processes. Businesses increasingly depend on digital technologies that are widely integrated into various business areas and processes (Eling et al., 2023). Usually, cyber risks refer to economic losses, reputational damage, lost clients, damaged systems, or business interruption. Financial institutions have significantly transformed their operations, by incorporating Artificial Intelligence (AI) and Big Data into the finance sector (Saeed et al., 2023). Daily, a vast amount of data is generated within the financial industry, encompassing everything from customer details to transaction histories (Ahmadi, 2024). Effectively tracking the security situation and correctly reporting it brings transparency and helps evaluate the conditions in the cyber security area (Fairford & Jembei, 2023). Financial institutions should implement a practical cyber risk evaluation framework to increase cyber security levels. Cyber risk assessment, management, or mitigation measures require additional resources – human resources, time, and financial investments (Kamiya et al., 2021). According to the World Economic Forum (2024) & European

Central Bank (2024), cyber risks have been recognised as one of the priority risks to the stability of the European financial system. To ensure business continuity and security, financial institutions must create new processes to assess the level of cyber security within the organisation (Patil et al., 2022). Currently, there is no tool to evaluate cyber security levels in financial institutions or any evaluation tools that only focus on the specific features of financial institutions.

Relevance of the Dissertation

Electronic financial services are an integral part of everyday life, so cyber risk is one of the newest and most dangerous for institutions in the financial sector. As the study conducted by the Bank of Lithuania (2023) showed, the possibility of cyber threats and the perceived impact on the Lithuanian financial system is one of the most pressing problems that should be identified as a priority in the coming years. In the European Union Directive on measures for a high standard level of cyber security across the Union (NIS2 Directive, 2023), a lot of attention is paid to data protection and cyber security. Therefore, a new approach to the evaluation of cyber security that is based exceptionally on financial institutions is necessary.

Research Object

The research object of this dissertation is cyber security assessment in financial institutions.

Aim of the Dissertation

The dissertation aims to develop a cyber security assessment tool that allows the evaluation of the cyber security level in a financial institution.

Tasks of the Dissertation

The following tasks are set to achieve the set goal:

1. To investigate cyber risks and cyber-security features and importance, identify the main areas of cyber security with indicators representing each area's most significant features, based on scientific literature analyses.
2. To establish a methodology for a tool that allows the assessment of cyber security in a financial institution.

3. To develop a unique questionnaire matrix to conduct an internal assessment of a financial institution's cyber security level based on the provided cyber security indicators.
4. To create a tool for cyber security evaluation in financial institutions by proposing a composite cyber security index as a final result.
5. To assess cyber security in selected financial institutions to practically verify the proposed composite cyber security index.

Research Methodology

The following scientific methods were used to complete the research goal:

- Critical analyses and systematisation of scientific literature provide the concept of cyber security, its features, and its importance in a financial institution.
- Global Cyber security cost calculator as a tool for evaluating the possible financial losses caused by cyber risks to financial institutions.
- Expert interviews to gather qualitative data for the evaluation of cyber security significance and specifying main cyber security indicators.
- Multi-criteria decision-making methods (Simple Additive Weighting (SAW), Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS)) for determining cyber risk significance and the weights of cyber security indicators.
- The OECD methodology for constructing a composite index, follows a ten-step process, including data selection, imputation, multivariate analysis, normalisation, and weighting.

Scientific Novelty of the Dissertation

The dissertation provides new results for the science of economics:

1. After completing comprehensive scientific literature analyses, four main areas of cyber security have been determined – legal, organisational, technical, and incident management, together with specific indicators that characterise each area exclusively for the financial institution.
2. By completing expert interviews and using MCDM methods, specific weights were established for 22 indicators, describing their importance in the general context of cyber security areas in financial institutions.

3. The original questionnaire matrix was created that allows financial institutions to evaluate each cyber security indicator internally.
4. The composite cyber security index for financial institutions was created. This new tool can be used as an effective method for cyber security evaluation in financial institutions.
5. From the perspective of the science of economics, a composite cyber security index serves as a new comprehensive tool for assessing and reducing cyber risks in financial institutions and can be used to plan investments in cyber security.

Practical Value of the Research Findings

A financial institution could use the developed and empirically tested original tool for cyber security evaluation in financial institutions to evaluate the organisation's cyber security level. Moreover, this proposed tool could be significantly helpful for identifying institutions' vulnerabilities and weak spots in specific areas. It could serve as a benchmark for improvement and investment allocation assumptions. The Composite cyber security index allows the evaluation and comparison of results in different institutions and enables the estimation of the general cyber security level in all financial systems.

Defended Statements

The following statements based on the results of the present investigation may serve as the official hypotheses to be defended:

1. The theoretical background for constructing a composite cyber security index is created by the systemic approach provided on cyber risks, and cyber security features and allows for determining the main cyber security areas and indicators specifically for financial institutions.
2. An original questionnaire matrix for internal cyber security level evaluation concerning all cyber security areas and indicators is a comprehensive and useful tool to assess cyber security in a financial institution.
3. The compiled model of the main cyber security areas, indicators, their specific weights, and internal evaluations of financial institutions allows for the creation of a composite index for assessing the level of cyber security.

4. The composite cyber security index is a suitable tool for assessing the cyber security level in a financial institution and for general comparison between different organisations.

Approval of the Research Findings

Four scientific articles have been published on the topic of the dissertation: 2 - in international peer-reviewed scientific journals, one of which is included in the *Scopus* database (Gavenaite-Sirvydiene & Miecinskiene, 2023a; Gavenaite-Sirvydiene & Miecinskiene, 2023b), which provides a citation index, and 2 - in proceedings of international conferences (Gavenaite-Sirvydiene & Miecinskiene, 2021; Gavenaite-Sirvydiene, 2022),

The results of the research performed in the dissertation have been published and presented by the author at two international scientific conferences:

- The 15th Annual Scientific Baltic Business Management Conference "Building Strategic Resilience in Times of Uncertainties". 2022, June 1, Riga, Latvia;
- "Contemporary Issues on Business, Management and Economics Engineering". 2021, May 13, Vilnius, Lithuania.

The author has also given four presentations at the Vilnius Gediminas Technical University doctoral seminars and one presentation at an international seminar in Latvia (BA School of Business and Finance).

Structure of the Dissertation

The dissertation is structured around three chapters. The first chapter of the dissertation is dedicated to analysing cyber risks and cyber security features. Also, it draws a deeper analytical understanding of the significance of cyber security, specifically in financial institutions. The dissertation's second chapter combines the methodology for constructing a cyber security index. Therefore, in this part, cyber security areas and indicators are provided, completed expert interviews and a structure for the cyber security index framework are provided. The third chapter presents a result – a composite cyber security index for financial institutions. It provides a deep-dive framework for evaluating cyber security areas and analysing possible vulnerabilities and strengths. Also, the results of three financial institutions' cyber security indexes are presented and compared. The dissertation contains 35 tables, 21 figures, 17 formulas and 163 references.

1

Theoretical Background of Cyber Risks and Cyber Security

This chapter introduces the analyses of scientific literature regarding general cyber security concepts and cyber risks. A deeper investigation is provided on specific features of cyber security, essential components of cyber risk definitions, specific cyber risks for financial institutions, cyber risk management significance and approaches, and legal issues of cyber security relevant to financial institutions. One scientific publication was published on the topic of this chapter (Gavėnaitė-Sirvydienė, 2022).

1.1. Concept and Features of Cyber Risks from a Theoretical Perspective

The financial services industry is related to the functions of financial flow management and customer data and relations. The main function of financial institutions is to aggregate and distribute public funds to support the implementation of national development and increase equity in development and its outcomes. Financial institutions are one of the foundations for economic growth and national stability to improve public finances (Santika et al., 2022).

Various types of risk are a crucial part of the general business environment. Several risk groups are identified: compliance risk, financial risk, operational risk, market risk, and strategic risk (Virglerova et al., 2021). Since people, internal systems, and business processes are all linked to financial institutions' operational performance, operational risk is one of the key risks that should be managed.

Various authors (Pengelly, 2016; Cebula & Young, 2010; Eling & Schnell, 2016) categorise cyber risk as a part of operational risk. The cyber risk could be classified as an operational risk because it is associated with the conduct of activities in cyberspace that threaten information assets, IT resources and technological assets, which may cause material damage to an organisation's tangible and intangible assets, business interruption or reputational damage (Strupczewski, 2021). Cyber risk can be identified whenever activities, tasks or functions are carried out in cyberspace, regardless of whether they fall under traditional risk categories such as strategic, market, credit, operational or legal risk (ISACA, 2009; Abdullayeva, 2023) (Fig. 1.1).

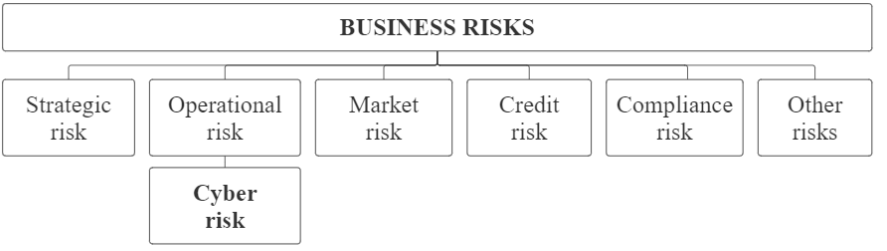


Fig 1.1. Cyber risks in the general business risk hierarchy (compiled by the author, based on ISACA, 2009; Strupczewski, 2021)

Cyber risk is related to various sources that can affect a company's or individual's technology assets, information databases or other online storage. Based on the Geneva Association (2018), cyber risk is the most significant challenge facing modern economies. It can be described as any risk from the usage of information and communication involving the deliberate attempt by computer criminals using the Internet to use the networks of computers, they have taken control of to alter, block or destroy computer systems, computer networks, data, or programs. Analysing the cyber risk concept based on the categories covered by insurance, cyber risk implicates the characteristics of property and liability risk together with operational and catastrophic risks (Eling & Wirfs, 2016). Cebula and Young (2010) indicated that cyber risk could be an operational risk to technology assets and internal information that may have consequences and affect the availability, confidentiality, or integrity of a company's internal systems and private information.

Financial institutions and insurance market regulators generally classify cyber-type risks as part of operational risk because they relate to technology and information assets. Therefore, cyber risk can be defined as an operational risk to technology assets and information that impacts information availability, integrity, and confidentiality (Chapelle, 2018).

Chavez-Demoulin (2015) pointed out that cyber risks can be divided into two general groups depending on the source of the risk: insider (financial damage, fraud, data, and identity theft by employees) or outsider (confidential information of the company money). As a result of these cyber risks, companies can lose confidential information and money and experience a loss of reputation, goodwill, and credibility.

According to Solvency (2009) document guidelines, cyber risks can be divided into four categories: technology and system failures, internal process failures, human actions, and external processes (Table 1.1).

Table 1.1. Categories of cyber risk (compiled by the author based on Solvency, 2009; Chapelle, 2018; Chavez-Demoulin, 2015)

Category	Definition	Factors
Act of people		
Inadvertent	Actions taken without harmful intent	Errors, mistakes
Intentional	Actions taken intentionally to cause harm	Fraud, theft, vandalism
Inaction	Failure to act in a harmful situation	Lack of skills and knowledge
Technology and system failures		
Hardware	Risks due to failures in manual equipment	Failure due to performance, capacity, maintenance
Software	Risks caused by programs, applications, operating systems	Security settings, coding, testing, configuration management
System	Failures as integrated systems do not perform as expected	Integration, design, specifications
Unsuccessful internal processes		
Process design	Failure due to poor process design or execution	Documentation, information flow, responsibilities, alerts, notifications.
Process control	Poor control of the process operations	Periodic review, process ownership, monitoring
Process support	Failure to deliver appropriate resources to support the process	Accounting, staffing, training, development

End of Table 1.1

Category	Definition	Factors
External processes		
Catastrophes	Human and natural events over which the organisation has no control	A weather event, fire, flood
Legal issues	Risks caused by legal arguments	Legalisation, regulations, litigations
Business issues	Risks caused by the changes in the business environment	Supplier failure, market condition, and economic causes
Service reliance	Risks arising from the organisation's reliance on external parties	Utilities, fuel, emergency services, transportation, and other suppliers

Jouini (2014) offers a different approach to classifying cyber risk. It is suggested that a threat is the adversary's target or what the adversary is willing to do to a system. It is also described as the opportunity for an adversary to attack a system. Therefore, a risk may be described in two prospects: techniques that attackers use to exploit the vulnerable components in the system or the impact that risk may cause on the company's assets. In this case, cyber risks may be classified by these approaches:

1. Classification methods based on attack techniques;
2. Classification methods based on attack impact.

Continuing the analyses of cyber risk classification, a proposed classification of cyber-attacks uses dimensions (Nirmala et al., 2023; Toch, 2018; Srivastava et al., 2024) (Fig. 1.2).

The goal of the attack is the first dimension for classifying cyber risk. Usually, it is closely related to how an adversary benefits from the attack, e.g., by stealing somebody's private information and selling it to other parties. The attack goals are divided into three different categories (Zhou, 2010):

1. Stealing information (e.g., private files, media files, data on private devices, and user credentials). This attack is mainly performed using malware or spyware.
2. It is primarily done by a virus program (Trojan, Botnet, Rootkit (Graziano et al., 2016)). It creates an environment for attackers to take complete control of the device.
3. Tracking user information. This applies to monitoring and collecting users' private, sensitive data Taking control of a system., such as activities, credentials, locations, bank account details, and other private information. This is achieved mainly by using remote mobile malware tools.

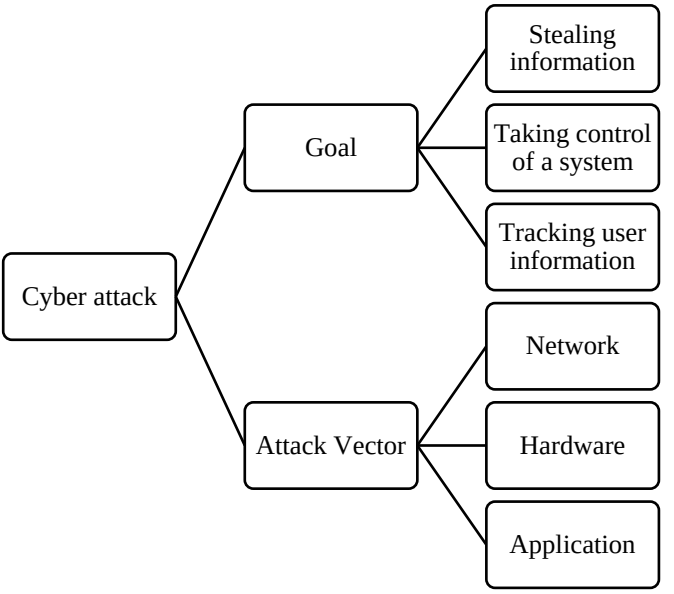


Fig. 1.2. Classification of cyber-attacks based on dimensions (compiled by the author based on Nirmala et al., 2023; Toch, 2018; Srivastava et al., 2024)

The second dimension in the classification model for cyber-attacks is the attack vector. This introduces the situation where the attacker exposes a company's vulnerability and maintains access to private computer systems and networks to perform harmful actions. Attack vectors may be classified into three different types:

1. Hardware Attacks. These attacks include backdoor creation, memory access and hardware tampering. The primary goal of these attacks is to modify the hardware to access private information and create a backdoor (Tehranipoor & Koushanfar, 2010) (installing an invisible program in the hardware) that can be used to regain access to the attacked system. Such hardware attacks can be applied to network appliances, surveillance, and industrial control systems.
2. Network Attacks. It is probable to aim the network protocol or the network device software; their goal is either denial of service or hijacking a network connection to steal sensitive data. Specifically, a common attack using network layer vectors is a denial of service (DoS) (Schweitzer et al., 2016).
3. Application Attacks. Phishing and client-side web attacks are most common at the application key point. These attacks target applications

such as e-mail services and web browsers because they are most exposed to the Internet. Regarding e-mail attacks, phishing is a fraud in which the attacker attempts to obtain sensitive information, such as login credentials and credit card numbers, by posing as a reputable organisation or individual via e-mail (Fette et al., 2007).

Nowadays, online attackers can use various methods to obtain the information or data they are interested in (Wu, 2015). All types of cyber risks are growing, and these are the most common and widespread types of cyber risk (Table 1.2).

Table 1.2. Types of cyber risks (compiled by the author based on Wu, 2015; Zhou, 2010; Fette et al., 2007)

Cyber Risk	Description
Ransomware	It is software that sits in a company's system to prevent employees from accessing critical information. Attackers then demand a ransom to restore access, often in cryptocurrency. However, the attackers may not regain access, and any information that is restored is still compromised. This threat is growing, especially as some cybercriminals are selling ransomware kits to people with limited computer skills.
Hacking	It refers to any attempt to access or compromise electronic systems, including the company's website, customer information databases, employee computers, or smartphones. This kind of attack can also refer to the more manual process of an individual hacker breaking into a system.
Malware	A shorthand term for malicious software, malware is software that is installed on a computer system and used to access data or sensitive information without the organisation's knowledge.
Malicious code	It is code or a link containing malicious files or programs. The code infects via downloads or attachments when visiting infected websites or in links sent via e-mail, social media, or text messages.
Social engineering or phishing	It is an attack in which the criminal impersonates a credible company to obtain personal information. Attackers may use official letterhead in e-mails, sophisticated websites, or phone calls to inquire about something that appears official. In some cases, the attacker may pose as a trusted company official, so it is important to investigate any instances of employees asking for sensitive information online.
Denial of service attacks	It occurs when employees fail to access standard computer systems due to a system overload caused by cyber criminals. Hackers flood the company's system with traffic until it can no longer handle the load, resulting in financial loss to the company. Attackers may use the opportunity to access information from that system or divert attention away from the attacked system.

End of Table 1.2

Cyber Risk	Description
Outsourced company access	If companies outsource services, they can increase their cyber risk by giving those companies access to networks and data. If cybercriminals can compromise the service provider, they may find a backdoor into a leading company's system and sensitive information.
Stolen or hacked employee devices	While protecting employees' computers may be at the top of the company's security list, other devices may not have the same level of protection. For example, hackers may target an employee's smartphone to access their e-mail or find sensitive information that has inadvertently been left unprotected. Stolen employee computers and devices can also put information at risk.
Malicious botnets	A botnet is a group of computers or systems that coordinate a task. While botnets can be used for website maintenance or other non-harmful purposes, attackers use them to coordinate a cyberattack, such as a denial of service, e-mail spamming, or malicious pop-up ads (Zhou, 2017).

The summary of cyber risk classification methods shows that there are two general ways of classifying cyber risk: based on the source of risk (human factor, internal causes, and external risk) and the tool used for cyber-attack (application, network, and software). All these risk types are very different from the fundamental ones as they arise from various sources and with other measures, but in general, they all conclude with the same result, i.e., the harm to the company's private information, IT assets, financial assets, and other operational matters.

Implementing cyber risk assessment measures is crucial to the successful reduction of the possibility of cyber risk occurrence. Generally, risk assessment enables cooperation with uncertainty in the business environment. Together with protecting what is valuable in the organisation, risk assessment and management encourage innovations and further development (Luburic, 2019).

A cyber-attack may have many different outcomes, e.g., loss of confidential data or customer information, network security issues, loss of customers because of a data breach or lousy press, financial loss from theft, product recall, lower share value, and business interruption (IBM, 2016). Considering all these possible outcomes, it is essential for the company to carefully evaluate potential threats and successfully implement an internal cyber risk management process.

The whole cyber risk assessment process is critical for establishing and implementing an effective cyber security management program, and the cloud plays a significant role in the business continuity field (Farid et al., 2023). A comprehensive comprehension of cyber risks is imperative to ensure that an

organisation's security measures are adequate in safeguarding against cyber threats (Santini et al., 2019).

Previous scientific studies on cyber security assessment mainly focused on one specific cyber security area but did not cover the whole set of cyber security fields (Aksu et al., 2017; Hartmann & Steup, 2013; Karabacak & Sogukpinar, 2005; Naumov & Kabanov, 2016; Hubbard & Seiersen, 2016). Prior research underlines the challenge of constructing dependable probabilistic models for cyber risk, given the complex array of stakeholders and events involved. Real-world applications often hinge on specific characteristics of the entities involved. For instance, employing a qualitative approach in risk assessment may yield robust controls for defending against malware; however, it does not ascertain the efficacy of these measures in mitigating actual malware attacks. Consequently, inaccurate prioritisation may lead to misallocation of resources, with significant investments directed towards areas of lesser importance while critical risk areas remain under-addressed.

According to Radanlieva et al. (2018), the general cyber risk assessment process could be categorised into these parts:

1. Risk identification strategy.
2. Risk estimation strategy.
3. Risk prioritisation strategy.

Current risk assessment methodologies, such as those based on Return on Investment (ROI) and Net Present Value (NPV), encompass diverse sets of criteria, such as the economics of privacy, optimal investment amounts, and risk aversion (Gordon & Loeb, 2002). Nevertheless, cyber risk encompasses facets beyond the financial costs associated with information security. Therefore, there is a need for a methodology that seamlessly integrates cyber risks with economic considerations. Since the motivation for cyber risk can extend beyond purely financial motives yet still result in economic implications, it is crucial to quantify this impact, focusing on averages and the most severe scenarios (Caralli et al., 2007).

According to the National Cyber Security Centre (2023), these are the main steps towards to cyber risk assessment and management:

1. Establish the context of risk.
2. Define the scope for risk assessment.
3. Evaluate assets and impact for assets.
4. Assess the threat.
5. Assess the vulnerabilities.
6. Estimate the likelihood.
7. Assess cyber security risk.
8. Communicate and document risks.
9. Prioritise risks and propose risk management actions.
10. Develop a risk treatment plan.

Emphasising risk assessment and management as an ongoing process is crucial. Neglecting this aspect would fail to promptly adapt systems, services, and security measures to address evolving technologies and emerging threats. Therefore, it is imperative to periodically revisit cyber security risk assessments and controls, mainly when significant changes occur (Ifinedo, 2023).

America's Cyber Defence Agency (2022) proposes these guidelines for cyber risk assessment (Table 1.3):

Table 1.3. Process guidelines for cyber risk assessment (compiled by the author based on America's Cyber Defence Agency Report, 2022)

No.	Step	Description
STEP 1	Identify and Document Network Asset Vulnerabilities	Analysing or cataloguing network elements and infrastructure, encompassing hardware, software, interfaces, and vendor access and services, aids in identifying potential threats. For instance, examining internal and external cyber procedures and interfaces (checking for default passwords), establishing data recovery procedures in advance, and reviewing access for each system are beneficial actions. This approach also facilitates comprehension of potential breach origins within the system.
STEP 2	Identify and Use Sources of Cyber Threat Intelligence	Several prevalent threats include but are not restricted to unauthorised access to sensitive information, the improper utilisation of data by an authorised user, and vulnerabilities in organisational security measures.
STEP 3	Identify and Document Internal and External Threats	Threats do not necessarily have to be external to organisations, as internal sources can significantly affect cyber security. Threat sources can come from inside an organisation; therefore, it is essential to identify internal processes. Employees, either accidentally or with malicious intent, can impact a network. By identifying internal and external threats and vulnerabilities, organisations can help anticipate a system breach and plan accordingly. For example, it is recommended to establish and consistently maintain a cyber incident response plan. Additionally, organisations can devise training and exercise initiatives to enhance cyber awareness and facilitate ongoing enhancement.

End of Table 1.3

No.	Step	Description
STEP 4	Identify Potential Mission Impacts	Information and communications technology is vital in critical infrastructure's daily operations and functionality. If these systems are compromised, the repercussions can extend to all users of the technology or service and systems beyond the organisation's jurisdiction. This assessment will evaluate the impacts on all system dependencies and shared resources in the event of a cyber incident. This evaluation is essential for containing a cyber breach across shared resources and can serve as a valuable reference when developing a response plan.
STEP 5	Use Threats, Vulnerabilities, Likelihoods, and Impacts to Determine Risk	Risk serves as a compass in crafting an incident response plan, yet it does not signify the definitive state of an organisation's cyber posture. Recognising that a cyber risk assessment is not a one-time event is essential. Instead, it is designed to continuously evaluate an organisation's cyber defences, which should be regularly updated as new technologies and methodologies emerge and are integrated.
STEP 6	Identify and Prioritise Risk Responses	An essential element of risk-informed decision-making for authorising officials involves comprehending their information systems' security and privacy stance and the standard controls accessible for those systems. Understanding the range of available responses to counter various cyber threats is a pivotal aspect of cyber risk assessment. Maintaining and regularly updating a roster of identified personnel and groups and their contact details is imperative to facilitate prompt response following a cyber incident.

Also, it is essential to emphasise the value of risk level evaluation. The assumptions during this process could be valuable for further cyber risk management actions (Fig. 1.3).

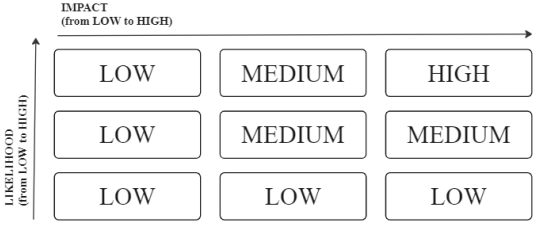


Fig. 1.3. Risk matrix to quantify the level of risk (compiled by the author based on America's Cyber Defence Agency Report, 2022)

Several factors should be considered when assessing risk levels, including (CISA, 2022):

1. Clarification of the assumptions underlying the categorisation of “high”, “medium”, and “low” risk levels.
2. Consistent and precise definitions of terms like “risk” and “threat”.
3. Identify assets, devices, and systems vulnerable in high-risk scenarios.
4. Analysis of the cyber threats targeting these assets, devices, and systems (See Steps 1 and 3).
5. Evaluation of the effectiveness of existing controls at each level in mitigating cyber breaches.
6. Assessment of the level of readiness attained by IT personnel to respond to cyber incidents.

Cyber and IT-related risks are often considered a subset of operational risks. They are frequently identified as significant threats to the financial system, as evidenced by research studies such as Kaffenberger et al. (2017) and Kashyap and Wetherilt (2019). However, these risks extend far beyond the financial sector, as indicated by the increasing interest in cyber security. In March 2017, G20 finance ministers and central bank governors recognised that “the malicious use of information and communication technologies (ICT) could disrupt critical financial services, both domestically and internationally, and undermine safety, confidence and financial stability”. Subsequently, in December 2018, the Basel Committee on Banking Supervision published a report highlighting various cyber resilience practices (Basel Committee on Banking Supervision, 2018).

A different approach to cyber risk assessment suggests that some methods are based on analysing user responses and the basis of their conclusions (National Institute of Standards and Technology, 2018). This classification method defines threats for network-dependent systems (Fig.1.4). Implementation of this approach includes designing different scenarios for cyber threats.

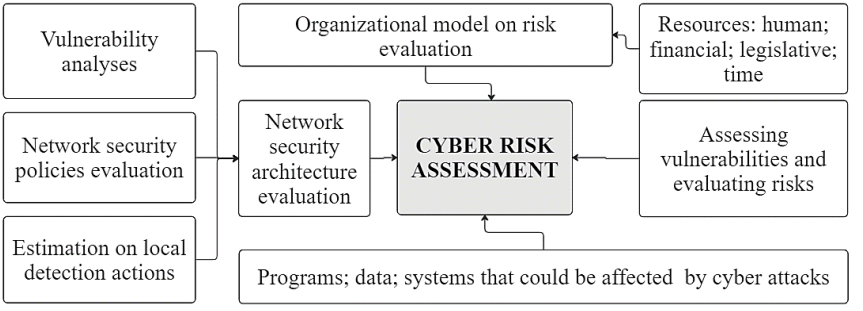


Fig. 1.4. Process of Cyber Risk Identification and Assessment (compiled by the author based on the National Institute of Standards and Technology, 2018)

This suggested risk assessment and management process is based on the relationships between different departments in the organisation. A big part of this model is dedicated to Network Security Architecture. It involves analyses of vulnerabilities, security policies, and event detection. All these parts are essential because they allow for proactive reactions to events, predict possible threats, and organise preparation, assessment, and protection measures (Johnson, 2013). Another essential part of this scheme is resources. They include all possible means that the risk evaluation process may require, i.e., human, financial, time, and legal resources. All possible resources may be calculated to implement an effective and fully functioning risk management protocol.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework is one of the well-known risk assessment frameworks. This framework offers flexible and structured guidelines for organisations to assess their cyber security risks and prioritise actions to reduce them. The NIST Cyber security framework has five major elements (Table 1.4).

Table 1.4. Elements of NIST Cyber security framework (compiled by the author based on The NIST Cybersecurity Framework 2.0, 2023)

Step	Description
Identify	Establish the organisation's baseline security strategy and evaluate risks.
Protect	Implement security tools to protect from identified threats.
Detect	Create and implement detection processes to verify cyber security incidents.
Respond	Develop and implement response action plans for identified cyber security incidents.
Recover	Create and implement plans to recover systems and data following a cyber security accident.

The NIST Cybersecurity Framework offers guidance to industry, governmental bodies, and other entities aiming to mitigate cyber security risks. It presents a taxonomy of overarching cyber security objectives, which can be adopted by organisations of any size, industry, or level of maturity to enhance their comprehension, evaluation, prioritisation, and communication of cyber security efforts. Notably, the Framework refrains from dictating specific methods for achieving these objectives; instead, it aligns with supplementary resources offering further insights into practices and controls conducive to realising these outcomes.

The ISO 27001:2013 standard could be named a framework for risk assessment. This standard provides a comprehensive approach to information

security management, including risk assessment and treatment requirements. ISO/IEC 27001:2022, as an internationally recognised standard to assist organisations in overseeing the security of their information assets. This standard offers a structured framework for establishing an Information Security Management System (ISMS) designed to safeguard the confidentiality, integrity, and availability of various corporate data sets, including financial records, intellectual property, employee information, and data managed by third-party entities.

Another approach to evaluating cyber security, according to Mettler (2011), is the cyber security maturity model. In general, maturity implies "an evolutionary progression in the demonstration of a specific capability or the achievement of a goal from an initial to a desired or normally occurring end state". Inadequate assessment of an organisation's cyber security maturity can also lead to underinvestment and financial losses (Strohmier et al., 2022).

Based on this view, maturity models are tools to evaluate improvement possibilities in the company. The maturity model enables the assessment of the organisation's current security situation (Le & Hoang, 2016). Therefore, the general functions of this model involve:

1. A possibility to assess the performance and identify a benchmark for best practice.
2. Detailed list of steps (road map) to achieve improvement.
3. Identification of obstacles and gaps by developing improvement plans.

The cyber security maturity model aims to explore and evaluate the current state of an organisation's preparedness to manage cyber risks and the level of implemented controls. Finally, it will assess the maturity level of the organisation. Each maturity level is based on a set of processes. Continuously, each method depends on the organisation's specifics, structure, operational issues, available resources, and personnel (Matari et al., 2021). Various experts in this field try to frame cyber security maturity models and attempt to collect best practices in consideration of capabilities, awareness, and the organisation's experience, empowering them to provide services efficiently without any disruption, protect private customer data and sensitive information, and follow the regulations and legal requirements. Therefore, it can be assumed that cyber security maturity models provide organisations with the capability to cyber security evaluation, planning, and manage risks (Acosta & Jahankhani, 2023).

According to Maglaras et al. (2020), maturity models mostly combine various components. Models mainly consist of clearly defined structures that are consistent with every step. The elements of models include different stages, attributes, and techniques. Maturity models measure an organisation's capacity for continuous improvement by qualitatively assessing maturity factors, such as people, processes, and technology (Mattler, 2011). As Lahrmann et al. (2011)

noted, they are widely used in management science and information systems development to assess institutions' capacity for continuous improvement.

In adopting the cyber security maturity model, it is essential to know that this process provides the organisation with guidelines for managing and mitigating cyber risks in its ecosystem. Teams should be aligned and processing to complete a perfectly working cyber security maturity model of various processes and measures (BitSight Technologies, 2023). According to BitSight Technologies research, these are best known and used frameworks for cyber security maturity models:

1. NIST cyber security framework.
2. ISO/IEC 27000:2018.
3. CIS 20.

The National Institute of Standards and Technology (NIST) provides a cyber security maturity model used by U.S. organisations. This framework involves a changing and improving view of risk and security measures that adopts a model to enhance and adjust research techniques strategy. The second broadly used framework, ISO/IEC 27000:2018, is the international standard (created by the international organisation ISO) to collect and describe best practices for cyber security, information security, and management of possible risks. This cyber security maturity model is commonly known and used in the European Union countries. It focuses on significant issues like technology, organisational processes, and employees (people) and indicates these three pillars as the main areas for cyber security maturity management. The third mentioned model is CIS 20. This model was created by the Centre for Internet Security (CIS) as a series of 20 crucial (critical) controls to protect an organisation's network from cyber breaches. This suggested model requires extreme attention to the processes built into organisations to manage cyber risks (Shaikh & Siponen, 2023).

These cyber security maturity frameworks can help mature security programmes, improve cyber hygiene and mitigate risk across a digital ecosystem. Organisations can follow a cyber security maturity model based on standard practices in their industry or among peers or may be required to adhere to a specific framework. Each provides examples of cyber security policies that can accelerate the work of security and risk teams to build effective programmes (BitSight Technologies, 2023).

Looking deeper into the possible structure of the cyber security model, the example of CMMC (cyber security maturity model certification) could be used. This is a tool created by the U.S. Department of Defence (DoD) to evaluate an organisation's cyber security maturity. This model contains five levels. The organisation defines each level as an established process and follows it with other implemented tools or practices. The following figure shows the relationships between these five processes across the CMMC maturity levels (Fig. 1.5).

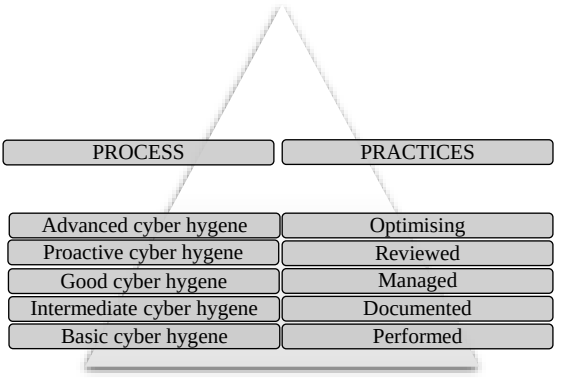


Fig. 1.5. Cyber security maturity levels (compiled by the author based on the U.S. Department of Defence, 2021)

In this model, five levels describe the organisation's development in the context of cyber security maturity. Level 1 reflects the main protection activities and only meets basic requirements. Level 2 is a transitional phase for the organisation to reach Level 3. The focus here is on replacing ad-hoc processes/practices with well-documented processes and corresponding regular practices. In Level 3, the focus is achieved with well-established processes and the implementation of all regular practices. Level 4 is also the traditional stage to improve and reach Level 5. The final Level 5 is reviewing and measuring existing practices to gauge effectiveness and enhance security to protect from cyber security threats. At this highest level, organisations are continually improving existing processes and practices. Defending against cyber-attacks would include noticing missing logs, verifying the integrity of security-critical software, responding in real-time to anomalous network activity, recording network traffic that crosses organisational boundaries, etc. (Strohmier et al., 2022).

To summarise, cyber security maturity models could help companies shape their cyber security actions and plans to improve cyber resilience and stability. As the European Union Agency for Cybersecurity (ENISA) concludes, the significant reasons to seek cyber security maturity are:

1. Cyber security evaluation (understanding and measuring the maturity of cyber security and comparing the company with the market benchmark).
2. Individual/personalised plan (specific action plan explicitly concluded by an organisation to improve cyber security situation).

The major areas that should be evaluated and impacted are people (evaluation of awareness and preparedness), technologies (implementing best detection and mitigation practices), and processes (specific guidelines to manage cyber risk in the organisation).

To summarise, evaluating and managing cyber risk constitutes the foundation of information security management yet poses a significant challenge for organisations due to uncertainties surrounding potential attacks, resultant risk exposure, and limited resources available for investing in mitigation strategies. An adequate cyber security risk assessment process must be closely aligned with the main business processes and requires, first of all, the involvement of the organisation's management, with experience and vertical competencies in risk and security, as well as appropriate qualified technical tools. In this respect, it is essential to implement a process of analysis and selection of the most relevant technical and operational solutions, with the help of highly specialised external consulting services, starting from the situation.

1.2. General Characteristics and Components of Cyber Security

Cyber security is becoming one of the most critical issues for companies willing to empower their growth and business success by using online technologies. The development of online services has transformed how people communicate, work and do business and has become critical to economic growth worldwide. These changes have created opportunities for corporations and small businesses worldwide to benefit from the convenience, efficiency and speed of online transactions and the exchange of data and other information. Still, together, they drastically increased the possibility of financial losses, data disclosure, and reputational issues that arise because of the failure of the company's cyber security policy (Glorin, 2023). It is not enough to know what cyber security is; it is also essential to consider why it is significant. As hackers and attackers implement new technologies and develop their tools for cyber-attacks, organisations and responsible employees should be aware of the possible threats, why their organisation needs to maintain security and how to do so (Assaf, 2008).

Cyber security could be described as a part of Information Security, which is a multidisciplinary area of study and professional activity focusing on safeguarding and protecting Information Technology against a variety of dangers and threats (Georgiadou et al., 2022)

Generally, cyber security is the concept of protection from cyber risks for all the systems connected to the Internet, e.g., software, online data, and hardware. It is the practice that helps businesses and individuals avoid unauthorised access to private computers, databases, and other information stored online (Chang, 2012).

The terms used to describe security aspects of information, the Internet, and digital devices have drastically changed in recent years. At the beginning of the 21st century, descriptions usually used in this context were "Information

Security", "IT Security", and "Computer Security". Although these terms were very well accepted and understood by professionals in this digital environment, the wider populace usually felt confused about the meaning of these concepts and terms, their differences, and their features (Apruzzese et al., 2023). However, with the rapid development of information technologies and online services, new terminology started to evolve and became known and popular with the term – cyber security (Schatz, 2017).

Cyber security could be described as a process of protecting all electronic devices and online storage (computers, mobile devices, servers, electronic systems, networks, online data, and cloud storage) from cyber-attacks (Advisen, 2015). An additional approach might suggest that strategy, policy and standards for the security of data and operations in cyberspace encompass the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resilience and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomatic, military and intelligence missions as they relate to the security and stability of the global information and communications infrastructure (NICCS, 2018). Accordingly, organisational cyber security is defined broadly as organisations' efforts to protect and defend their information assets, regardless of the form in which those assets exist, from internal and external threats to the organisation (Dalal et al., 2021). In other words, it is electronic information security or security of information technology. According to Johnson (2013), the term cyber security implicates the relation between the impact and frequency of an attack. It can usually be measured during the risk management process. Stubley (2013) has taken a different point of view on this issue and offers to simplify the definition of cyber security to information security based on a short analysis of the cyber component defined as the use of information technology and computers. On the other hand, Schatz et al. (2013) proposed a new approach and claimed that cyber security must be defined using cyber risk as a significant component, concluding that cyber security is a sub-discipline of information security. As the British Standards Institute (2014) claims, cyber security can be described as a collection of policies, security codes, safeguards, tools, instructions, approaches for risk management, training practices, assurance, and technologies that can be used to protect the online (cyber) environment, assets, and data of an organisation.

Fredrick Chang (2012), former Director of Research at the National Security Agency in the USA, has suggested the interdisciplinary definition of the cyber security concept, suggesting that the science of cyber security offers many possibilities for security improvements based on a multidisciplinary approach because cyber security is about an adversarial engagement of businesses. Fundamentally, humans (or businesses) must defend machines or assets that are attacked by other humans using machines. So, in addition to the critical traditional

fields of computer science, electrical engineering, and mathematics, perspectives and different approaches are needed. According to DHS (2014), cyber security is the activity, process, ability, capability, or state that protects information and communications systems and information against damage, unauthorised use or modification, or exploitation (Fig. 1.6).

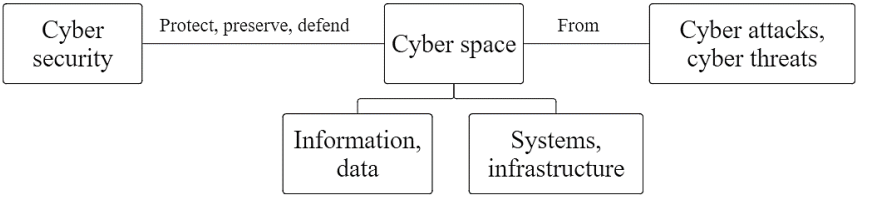


Fig. 1.6. Definition of cyber security (compiled by the author based on the DHS National Preparedness Goal, 2014)

Oxford University Press (2014) suggests that cyber security should be considered a state of being protected from unauthorised use or access, criminal intervention, or the measures taken to avoid these situations.

In describing the concept of cyber security, general characteristics and indications can be provided (Kianpour et al., 2022):

1. The ability to secure or defend the business environment from cyber-attacks.
2. Preventing the integrity and accessibility of information confidentiality in the business environment.
3. All measures and activities should be aimed at users and the protection of cyberspace.
4. Prevent risks and possible damage to protect and, if necessary, restore information, data, online storage, electronic communication systems and services.

The presented schematic view of the cyber security concept shows that cyber security aims to protect cyberspace (including information and infrastructures) from any cyber threat or cyber-attack. Institutions use the guidelines and tools associated with cyber risk management processes to protect the confidentiality, integrity, and availability of data and assets used in cyberspace. The framework includes guidelines, policies, and collections of safeguards, technologies, tools, and training to ensure the protection of the business environment.

According to Georgiadou et al. (2022), Walls (2013), and Galinec (2018), cyber security could be defined as the governance, development, management, and use of information security and operational technology security tools to achieve regulatory compliance, defend assets, and compromise adversaries' assets (Fig.1.7).

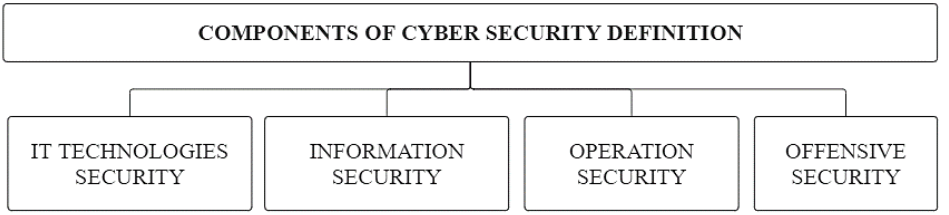


Fig.1.7. Components of the cyber security definition (compiled by the author based on Georgiadou et al., 2022; Walls, 2013; and Galinec, 2018)

Cyber security is a set of practices incorporated into information security, information technology security (IT), operational technology security (OT) and offensive security. Based on this point of view, cyber security uses the tools and techniques of IT security, OT security and information security to minimise vulnerabilities and provide system integrity and access only to authorised users. In this context, offensive security should be perceived as the process or approach to protecting computer systems, networks and individuals from cyber-attacks. Offensive security tools and measures are concentrated on seeking out the attackers and, in some cases, attempting to disable or at least disrupt cyber-attacks.

Craigen (2014) suggested this definition of cyber security: "Cyber security is the organisation and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights". Also, the author deconstructed this definition to explain it in more detail. The organisation and collection of resources, processes, and structure are indicated as a capture for multiple dimensions and specific complexity of cyber security, which may be interactions between humans and systems. Protection of cyberspace and cyberspace-enabled systems in the definition reflects the broader meaning of protection, including intentional, non-intentional, natural hazards and all other possible threats. Moreover, this aspect involves the traditional understanding of cyberspace and systems that are usually not discussed, such as cyber-physical systems and computer control systems. The protection point in this definition refers to the protection of all assets and information within cyberspace and any connected systems.

After reviewing and analysing the definitions proposed by different scientists to describe cyber security, a summarised description can be suggested: cyber security is the actions and approaches connected with security risk management processes followed by companies to protect the integrity, confidentiality and availability of their information, sensitive data assets and other property allocated in cyberspace. This cyber security concept involves policies, guidelines, training

programs, and other tools to ensure the highest level of protection for the company's cyber environment and its users.

Identifying the most relevant and accurate definitions of cyber security allows for the collection of the critical parts of this concept. The following model was built to better understand the main parts of the cyber security concept (Fig.1.8).

As the figure shows, cyber security is a complex concept. Dividing keywords from cyber security definitions into groups allows for a better understanding of their specifics and evaluation of the most essential components. The main parts of this concept could be separated regarding the process type or involved parts. To begin with, integrity, availability, and confidentiality are the expected values of a company that implements or runs a cyber security process. The organisation, user, and company part indicate that cyber security cannot be separated from the human factor; it requires the indication of the affected party – the organisation, company, or at least a user of online services. The other part, which involves environment, protection, and technology, describes the background of this concept because cyber security is closely related to technologies, their protection, and, in general, creating a safe environment (Li, 2021).

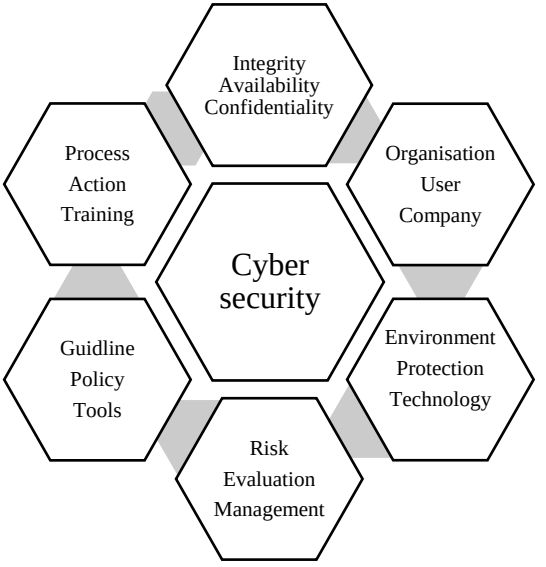


Fig.1.8. Cyber security concept (compiled by the author based on Galinec, 2018; Li, 2021; Zwilling et al., 2020)

The risk, evaluation, and management part shows that the cyber security process is a target for avoiding potential risks, evaluating possible threats and

losses, and empowering to create a strategy for cyber risk management. Furthermore, guidelines, policies, and tools are the technical part of the cyber security description and indicate an action plan, possible instruments for risk evaluation and management, and the guidelines that the company should follow in case of a cyber-attack. Finally, the last part of this concept – process, action, training – shows that cyber security, in general, is a process where a company and its employees must be involved in required safety processes, be aware of possible actions, and have relevant training courses (Singh et al., 2023).

The areas related to cyber security in the organisation could be divided into separate dimensions at the organisational and individual levels (Fig. 1.9).

This proposed model defines two levels: the organisational level is meant to involve factors related to IT infrastructure, operations, procedures, and guidelines, while the individual level is focused on the human factor, employee attitudes, and the impact of internal behaviour. This idea of cyber security areas combines external and internal factors related to cyber security issues in the organisation.

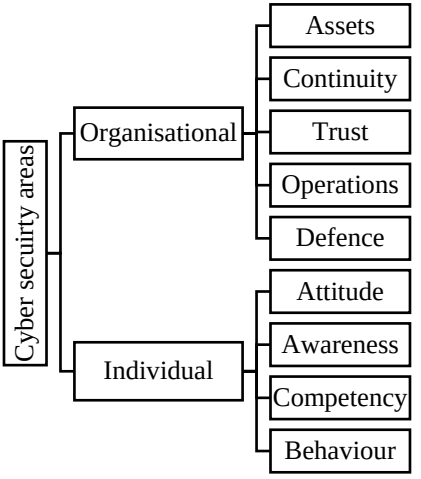


Fig. 1.9. Cyber security areas (compiled by the author based on Georgiadou et al., 2022; Kamiya et al., 2021)

By analysing combinations of policies and practices of cyber security usually implemented and practised by businesses, these major practical areas may be defined (Fig. 1.10).

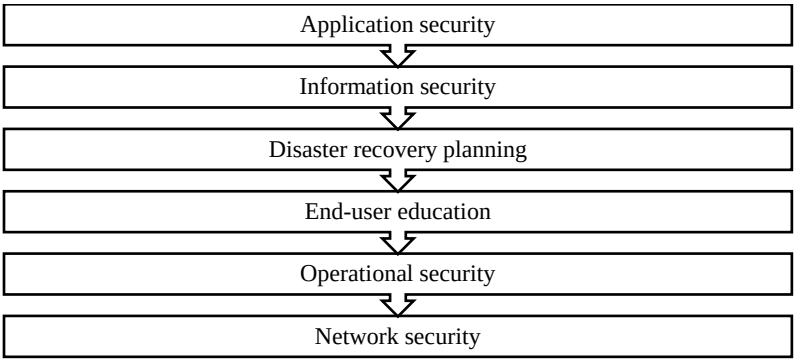


Fig. 1.10. Major areas of cyber security (compiled by the author based on Jitendra, 2017; Kartikey, 2014)

Application security is one of the significant parts of cyber security. It refers to adding security measures and tools within applications used by companies as a product for their customers to avoid cyber-attacks. It safeguards websites and web-based applications from different types of cyber security threats. The most common application threats or vulnerabilities can be identified as Denial of Service (DoS) attacks, data encryption, and data breaches. Application security is the use of such tools as software, hardware, or other procedural utilities to secure applications from external cyber threats. Application security includes measures or countermeasures that are implemented during the development lifecycle process to protect applications from threats that can be introduced through flaws in the application design, development, deployment, upgrade or maintenance, or in any other way disrupt the smooth performance of the application (Kartikey, 2014; Jitendra, 2017).

Information security reflects the process and methodology of preventing unauthorised access, use, disclosure, disruption, modification, or destruction of sensitive, personal, or private information. It is a set of business strategies for managing the processes, tools and policies crucial for ensuring the safety of sensitive information. Generally, strategies and management policies for information security are created around the primary goals, such as ensuring confidentiality, integrity, and information availability. These information security targets ensure that sensitive information can only be disclosed to authorised parties and confidentiality of information is guaranteed; they also prevent unauthorised modification of data that creates integrity and, finally, ensure that data can be accessed by authorised parties when requested, reflecting the information availability.

A Disaster Recovery Plan is a plan to ensure business continuity, together with management processes and procedures describing how the business should operate and resume quickly after a cyber threat. Usually, such a plan indicates the most critical applications crucial for keeping an organisation active (Walls, 2013). While creating the disaster recovery plan or business continuity guidelines in this context, it is essential to consider these issues (Vanichchinchai, 2022; Tómasson, 2022; Jitendra, 2017):

1. Financial budget.
2. Resources.
3. Technology.
4. Administration.
5. Hardware.

Operational security is a risk management and analytical process that identifies an organisation's critical information and involves developing a protective mechanism to ensure the security of vital information. To create an effective operations security program, first, the information and data that are considered sensitive should be defined. Furthermore, possible threats should be determined, and vulnerabilities in the context of cyber security should be analysed.

Network security is another element of the cyber security area, which can be described as preventing and protecting against unauthorised access to computer networks. It involves a combination of rules and specific configurations to control and monitor unauthorised access. It is important to note that network security includes hardware and software technologies.

The last component of general cyber security areas is end-user education. Currently, users are becoming one of the highest risks for a company's cyber security; therefore, educating end users is supposed to become one of the top priorities for businesses to ensure information security, cyber security, and business continuity.

To prevent and manage cyber threats, it is essential to understand that cyber security is a wide range of tools, methods, and practices. The leading five components that can help to create a broader view of what the cyber security concept involves (Elkhannoubi, 2015; Alghamdie, 2021; Abdallah, 2018; Mijwil et al., 2023):

1. Critical infrastructure. It involves traffic lights, electrical grids, water plants, hospitals, national security, and telecommunications. These are critical infrastructures related to cyber systems that every society relies on and depends on. Whereas the organisation is responsible for one of those critical infrastructures, it is crucial to identify the vulnerabilities and take protective action against them. For other organisations, it is vital to be prepared for disaster recovery, backup, or business continuity plans

in case an attack occurs under one of the critical infrastructure organisations.

2. Cloud security. It is becoming a more critical part of cyber security because businesses keep moving to cloud solutions. A wide range of solutions to create cloud security are available.
3. Internet of Things (IoT). It involves all devices that are connected to the network. Usually, these devices do not include security or are very weak. Therefore, the Internet of Things might be a possible source of cyber-attacks.
4. Network security is one of the critical parts of cyber security. Proactive network security should protect against hacker attacks and malicious intentions. It usually involves a firewall, antivirus software, behavioural analytics, and access control.
5. Ongoing employee training. The final part of cyber security is the education of employees. Employees are a significant part of the company and the company's ability to prevent business from cyber-attacks and incidents. People are often the primary target of cyber attackers as they are easily accessed via e-mail and social engineering attacks. To ensure cyber security, employees must feel confident about recognising cyber-attacks and how to reach them. Employees should receive training and education sessions regularly to prevent cyber-attacks via human factors.

To correctly evaluate the importance of cyber security, it is necessary to examine the magnitude of cyber-attacks and the consequences of cyber-crime. As an integral part of its cyber claims handling process, international reinsurer Chubb tracks the critical metrics of cybercrime: the actions that caused the cyber loss, the factor that caused the cyber incident (external or internal), and the number of areas involved or affected. These metrics are analysed alongside general trend data and help predict possible cyber events and losses, assessing exposure and mitigating consequences (Chubb, 2020). As noted above, cyber security in financial institutions is critical to sustainable, safe and successful business continuity.

Since 2020, cyber risks have become even more relevant due to the global pandemic (COVID-19). The pandemic has resulted in many employees working from their homes. Employees should improve their awareness and knowledge of probable cyber incidents while working remotely to protect the work environment. For these reasons, financial institutions must organise training effectively and proactively, and provide self-education tools and other measures to raise cyber security awareness.

The global COVID-19 pandemic has brought many challenges to financial institutions. They are at the forefront of responding to cyber threats. In the context of the pandemic, the provision of financial services changed drastically. The number of operations, actions and financial services offered only online increased;

many employees had to adapt to working from home (WFH). Moreover, these new circumstances are closely related to personal data, human privacy and security issues, making them one of the most attractive targets for cyber attackers (Harjinger, 2021). With the extraordinary impact on society's daily life and habits, the pandemic has created the conditions for new cybercrimes in households and businesses. The increase in uncertainty and fear in society led to many cyber-attacks.

During the global pandemic, the Crown Prosecution Service (CPS) in England described cybercrime as an umbrella term involving two types of illegal activity: cyber-dependent crimes and cyber-enabled crimes (Fig. 1.11).

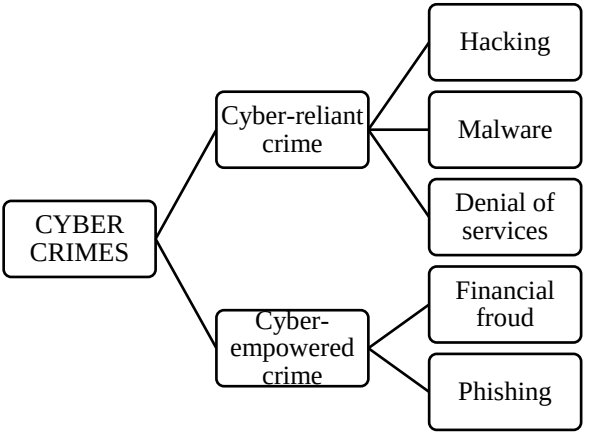


Fig. 1.11. Cyber-reliant and cyber-empowered crimes (compiled by the author based on CPS, 2020)

Cyber-reliant crimes can only be committed using IT technology and devices. In addition, these devices are used both as a tool to commit a crime and as a target of the same crime. For example, they create and distribute malware for financial gain and generate hacking tools to steal financial resources. Cyber-enabled crimes are traditional cybercrimes such as personal data theft and cyber-enabled fraud. This type of cybercrime does not rely on networks or computers. Still, it is created or designed using Internet technologies and, e.g., based on financial objectives – intellectual property crime or fraud, offensive communication, and bullying (CPS, 2020).

It is essential to identify new types or methods of cybercrime and to determine the possible consequences of cyber-attacks in the global pandemic. Cyber security issues during the pandemic could be categorised into direct and indirect effects (Fig. 1.12) (Ferreira et al., 2021).

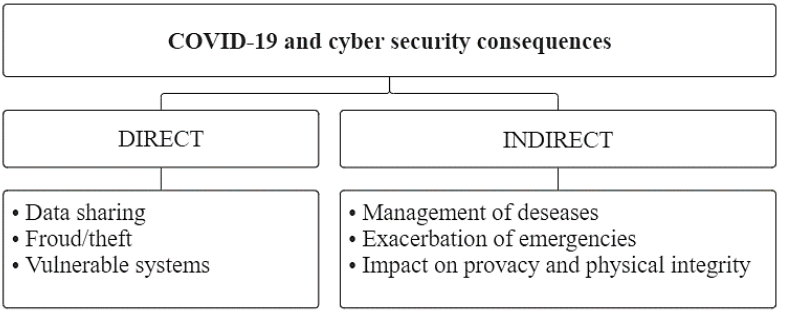


Fig. 1.12. Direct and indirect consequences of COVID-19 on cyber security (compiled by the author based on Ferreira et al., 2021)

When analysing the direct impact of the pandemic on cyber security, the issue of data sharing is one of the most pertinent, as protecting sensitive data and private information is essential but difficult to achieve. Various applications involve data sharing and collection of personal information, but users are not provided with adequate risk assessment and management tools. In addition, a user's lack of cyber security awareness can lead to cybercrime due to installed and used data-tracking applications. On the other hand, these apps may have technical security vulnerabilities (United Nations Office on Drugs and Crime, 2021). There has also been a dramatic increase in false information about pandemics. The aim of these attacks is usually financial fraud or data theft. In addition to the private use of online technologies, many public systems have become targets for cybercriminals. Some public institutions and private companies were unprepared for such circumstances and did not implement proper security measures or protocols. As a result, the risk of a cyber-attack while using these systems increased significantly during this period.

Researching the indirect costs of COVID-19 towards cyber security, one of the new options for hackers is the online pages or platforms used for health services and treatment of diseases. The cyber security evaluation systems are not ready to ensure adequate control and protection of personal data and other sensitive information. Because many people were isolated at home, insecure online communication became another severe consequence of COVID-19. A considerable part of the infrastructure was not adequately secured. Required precautions were not taken, and cyber security integrity did not ensure the safety of personal data and other information in virtual space.

The COVID-19 pandemic created remarkable and unique social and economic circumstances that cyber criminals were exploiting. Changes to working practices and socialisation meant people spent more time online. In addition, unemployment rates increased, meaning more people were sitting at home online, and some of these people likely turned to cyber crime to support

themselves (National Bank of Lithuania, 2021). The combination of increased cyber-attacks and cyber crime implies that there may be implications for policing worldwide – law enforcement needs to ensure that it can deal with cyber crime (Collier et al., 2020). COVID-19 created several challenges to business operations, resulting in rapid change. However, the necessity for relevant cyber security measures and regular review of the threat area did not change; it became more important.

Cyber risks come in many forms, from opportunistic or organised threat actors to inadvertent or accidental security failures. These risks are more acute in times of societal and organisational vulnerability. As the amounts and sophistication of cyber-attacks increase, institutions, especially those with national security, health or financial data, must take action to protect sensitive business and personal data.

Therefore, cyber security connects tools, methods, skills, and strategies to improve information, data or asset security, and risk management and provides feedback for information availability, integrity, or confidentiality (ISACA, 2014). Cyber security may be a matter of technological choice as it affects different parts of an organisation, such as legal, operational, or technological solutions. Thus, an effective cyber security strategy requires the high-level involvement of various organisation departments.

1.3. Legal Regulations and Data Security Framework for Financial Institutions

In the European Union, most member states have various methods to regulate the protection policies for critically important infrastructures and mostly different levels of cyber security and preparedness for cyber risks. These differences among EU countries are recognised as weaknesses and vulnerabilities in cyber security. The first official regulation document provided by the EU Commission was an NIS Directive, put into effect in November 2016. The general purpose of this Directive was to increase cyber security in the EU. First, the NIS directive was created to improve and empower cooperation and communication between members on cyber security and cyber risks. Second, the only way to create synergy among member countries was to implement the tool (ENISA, 2023)

The NIS Directive lists obligations to European Union member states regarding cyber security. Specifically, it implicates responsibilities for all countries (NordLayer, 2023):

1. To implement a national strategy for the security of networks and information systems.

2. To develop security and reporting requirements for operators and suppliers.
3. To designate National Competent Authorities, Single Points of Contact and CSIRTs with responsibilities related to the security of networks and information systems.

In addition, the NIS directive obligates the EU to take these actions:

1. Establishment of a Cooperation Group to support and facilitate strategic cooperation and exchange of information between Member States and to develop trust and confidence between them.
2. Establish a network of Computer Security Incident Response Teams (CSIRTs) to develop trust and confidence between Member States and to promote rapid and effective operational cooperation.

The NIS Directive sets out a wide range of network and information security requirements applicable to DSPs – Operators of Essential Services and Digital Service Providers. The "essential service providers" referred to in the legislation include companies in the energy, transport, banking, financial market infrastructure, healthcare, drinking water supply and distribution, and digital infrastructure sectors. The NIS Directive requires each EU Member State to draw up a list of organisations in these sectors that are considered to be essential service providers (ENISA, 2023).

The NIS Directive involves different requirements for responding after an incident, technical security issues, and implementation based on the risk. The requirements are designed to improve cross-border cooperation in information and network security and foster a culture of risk management (NIS Directive, 2023).

European Union Security Network. To improve cooperation between member states, the Directive indicates the creation of a network of Computer Security Incident Response Teams (CSIRTs) in every EU county for cross-border collaboration, cyber security monitoring, reporting, and incident response. CSIRTs should also have the necessary equipment and resources for resilient and secure infrastructure. Basic tasks for CSIRTs are monitoring national security incidents, preparing early warnings and announcements, and providing reports and analyses about cyber security and actual risks (NIS Directive, 2023).

Member State Strategy. EU member states have to integrate a national cyber security strategy that defines security objectives and relevant policies and regulations necessary to implement the Directive. The Directive requires each strategy to include a governance framework, response and recovery measures, plans for public and private sector security cooperation, security awareness training programmes, risk assessment plans and lists of persons and organisations involved in the strategy (NIS Directive, 2023).

Cooperation Group. Additionally, other bodies established by the NIS Directive are given a further mandate to establish a Cooperation Group. This group's primary objective is to facilitate collaboration on cyber security among Member States. Comprised of representatives from Member States and the European Union Agency for Network and Information Security (ENISA), with a member of the European Commission serving as the secretariat, the Cooperation Group is tasked with planning, steering, and monitoring the implementation of the NIS Directive. Key responsibilities of the group include guiding the newly established CSIRTs network, assisting Member States in identifying services to be classified as "operators of essential services", engaging with relevant entities on security incidents and concerns, sharing best practices in security, and enhancing awareness of cyber security within the EU (NIS Directive, 2023).

Incident Reporting. Organisations meeting the criteria to be classified as DSPs under the Directive are obliged to enact a range of technical and operational risk management measures. They are also mandated to adhere to the Directive's incident reporting procedure, necessitating prompt notification to CSIRTs and other pertinent entities about any significant security incidents encountered without undue delay (The official portal for European data, 2018).

It is critically important for organisations to understand the possible methods that might be used against the sensitive data they possess. Various types of information and data are likely to be considered sensitive information depending on the industry and business type, but mainly, the description of "sensitive information" should involve anything that is expected to be under strict protection (General Data Protection Regulation, 2016). Five examples of information are recommended to be considered sensitive (Table 1.5).

Critical components of financial institutions' data can be classified as sensitive information, encompassing intellectual property, financial records, personal data, or other types of data whose unauthorised access or exposure could result in adverse outcomes for the owner. Daily, organisations and companies transmit sensitive data and information across networks and between various devices to deliver services or conduct business; in such contexts, cyber security emerges as a discipline or methodology for safeguarding information (Tikkinen-Piri et al., 2018).

Table 1.5. Types of sensitive information (compiled by the author based on Wu, 2015; GDPR, 2016)

Type	Description
Customer information	Information such as customer names, residential addresses, payment card details, social security numbers, e-mail addresses, application attributes, and any other data enabling the direct or indirect identification of an individual.

End of Table 1.5

Type	Description
Employee data	Employee data resembles customer information, encompassing details such as employee names, addresses, social security numbers, banking information (for payment processing), usernames, passwords utilised for company access, or data linked with credential verification. This constitutes sensitive information, underscoring the importance for organisations to securely store it.
Intellectual property & trade secrets	Almost every company maintains proprietary data within their network, with a third-party entity, or within their document management system. This may include code for software developers or schematics for hardware developers. This instance of sensitive information may also encompass product specifications, competitive research, or any data covered by a non-disclosure agreement with a vendor.
Operational & inventory information	This instance of sensitive data encompasses generalised business operations or inventory data. Businesses involved in physical product sales typically prefer to keep their sales figures confidential and inaccessible to competitors. If revealed, sensitive data does not always pertain to personal or individual information but rather company-wide data that could affect business decisions, reputation, and operations.
Industry-specific data	Depending on the sector in which the institution operates, there might be particular instances of sensitive information that require protection. For instance, retail businesses must prioritise safeguarding customers' payment details, while healthcare institutions should emphasise the protection of digitally stored medical records and medical research data.

Cyber security and cyber resilience regulation initiatives and directives across the European Union members may be summarised with this list (European Union Cybersecurity Policies, 2020):

1. Network information security directive requires national cyber security management plans for critical sectors.
2. European Banking Authority (EBA) information and communication technology (ICT) guidelines provide supervisory requirements for potential operational risks and risk assessment models.
3. EBA governance guidelines involve business continuity planning and cover informational technology outsourcing risks.
4. General Data Protection Regulation (GDPR) lists requirements for data breach reporting and indicates associated fines for businesses in non-compliance situations.

5. European Central Bank (ECB) initiatives include incident reporting for financial institutions, testing the resilience of banks, and growing supervisory interest and actions.

European Central Bank has made significant progress in recent years in developing its involvement in and understanding of cyber security issues. In 2014, the ECB established a Single Supervisory Mechanism (SSM) so that supervisors could explore and study the best cyber security practices among countries. Also, the ECB has undertaken the function of information gathering to better understand cyber security issues at individual and financial systemic levels. Finally, the ECB uses its experience and knowledge to develop measures and tools for better addressing cyber risks (Table 1.6).

Table 1.6. European Central Bank Measures on Cyber security Management (compiled by the author based on Deloitte, 2018)

Banking supervision	Financial market infrastructure (FMI) oversight.
1. Framework for cyber incident reporting 2. Developing cyber risk management methodologies 3. Information technology risks are evaluated as a part of the operational risk component and involved in the review and evaluation process. 4. Information technology risk is included as a significant criterion for bank authorisation decisions	1. To better understand FMI cyber connectivity, an analytical benchmark and methodology were developed. 2. European Union team for testing and monitoring interconnectivity and development 3. Creating a Euro Cyber Resilience Board and expecting public-private cooperation through the establishment.

To summarise, financial sector companies are exposed to several possible cyber-attacks, which require consistent efforts and input to keep operating securely and under compliance regulations. Cyber risks have become more complex in recent years, and their impact could range from very low to very high. Therefore, compliance with supervising institutions has become increasingly important in the financial services industry. It is a tendency that is likely to continue or even grow due to the fast development of information technologies, online financial services, and mobile applications.

The objective of the EU Cyber Security Strategy is to foster resilience against cyber threats and to guarantee that both citizens and businesses can enjoy the advantages of dependable digital technologies (The Cyber Security Strategy, 2022). The accelerated digitalisation of society, exacerbated by the COVID-19 crisis, has broadened the scope of threats and introduced fresh challenges, necessitating tailored and inventive solutions. The frequency of cyber-attacks is

on the ascent, with more sophisticated attacks originating from diverse origins both within and beyond the EU.

Therefore, the EU should take the lead in fostering secure digitalisation efforts, establishing norms for top-tier cyber security solutions and standards applicable to vital services and critical infrastructures, and promoting the advancement and deployment of innovative technologies. Governments, businesses, and citizens share the responsibility of ensuring a cyber-secure digital transition. The strategy delineates how the EU can leverage and enhance its array of tools and resources to achieve technological sovereignty. Additionally, it outlines avenues for collaboration with global partners who uphold values such as democracy, the rule of law, and human rights (Greenleaf et al., 2017).

The acquisition of the EU's technological sovereignty must rest upon the resilience of all interconnected services and products. Collaboration among the four cyber communities – those involved in the internal market, law enforcement, diplomacy, and defence – needs to intensify to foster a collective awareness of threats. This collective readiness should enable a unified response to emergent attacks, amplifying the EU's efficacy beyond individual contributions.

The strategy addresses the security of essential services like hospitals, energy grids, railways, and the expanding array of interconnected devices in homes, offices, and factories. It endeavours to cultivate joint capabilities to counter major cyber assaults and delineates plans for global partnerships to uphold international security and stability in cyberspace. Moreover, it elucidates how a Joint Cyber Unit can mount the most effective response to cyber threats, utilising the combined resources and expertise of member states and the EU (Ardic et al., 2011).

The main aim of the strategy. The new strategy seeks to guarantee a global and accessible Internet while establishing robust safeguards against risks to both security and fundamental rights within Europe. Building upon the advancements made in previous strategies, it presents tangible proposals for implementing three primary instruments: regulatory measures, investment strategies, and policy initiatives (Cavelty & Smeets, 2023). These instruments will target three key areas of EU action:

1. Enhancing resilience, technological sovereignty, and leadership.
2. Strengthening operational capabilities to prevent, deter, and respond effectively.
3. Fostering cooperation to promote a global and open cyberspace.

The EU is dedicated to backing this strategy with an unparalleled investment in the EU's digital transformation over the forthcoming seven years, marking a quadruple increase from prior investment levels. This underscores the EU's dedication to its fresh technological and industrial policies, as well as the recovery agenda.

The strategy outlines how the EU can utilise and fortify all its tools and resources to achieve technological sovereignty and strategic autonomy. Additionally, it elucidates how the EU can enhance its collaboration with global partners who uphold shared values of democracy, the rule of law, and human rights. This strategic autonomy needs to be founded on the resilience of all connected services and products. All four cybercommunities – those concerned with the internal market, law enforcement, diplomacy, and defence – need to work more closely towards a shared awareness of threats. Moreover, they must be ready to respond collectively when an attack materialises so that the EU can be stronger than the sum of its parts (European Commission, 2020).

Numerous fresh strategic initiatives have been unveiled, encompassing an EU-wide Cyber Shield comprising Security Operations Centres equipped with AI and Machine Learning to identify early indicators of impending cyberattacks, enabling proactive measures to mitigate damage. Additionally, a Joint Cyber Unit will consolidate all cyber security communities to foster shared threat awareness and collective responses to incidents and threats. Furthermore, European initiatives aim to enhance global Internet security, including regulations for a public EU domain name system resolver service to guarantee a Secure Internet of Things (Ardic et al., 2011).

The strategy initiates enhanced and intensified cyber dialogues with third countries, as well as regional and international organisations, such as NATO, along with a Program of Action within the United Nations aimed at addressing global security concerns in cyberspace. Additionally, it proposes a bolstered EU cyber diplomacy toolbox to prevent, deter, and respond effectively to cyber-attacks.

In the 2021–2027 Multiannual Financial Framework, EU funding for cyber security is earmarked under the Digital Europe Programme. Simultaneously, funding for cyber security research is anticipated under Horizon Europe, with a special emphasis on supporting SMEs. This allocation could total EUR 2 billion, supplemented by investments from Member States and industries (European Defence Fund, 2020).

The European Defence Fund (EDF) is set to provide backing for European cyber defence solutions as an integral component of the European defence technological and industrial base. Cyber security is encompassed within external financial instruments aimed at supporting our partners, particularly through the Neighbourhood, Development, and International Cooperation Instrument. The Strategy aims to fortify Europe's collective resilience against cyber threats and ensure that all citizens and businesses can fully avail themselves of trustworthy and dependable services and digital tools. Whether it pertains to connected devices, the electricity grid, banks, aircraft, public administrations, or hospitals

frequented by Europeans, they deserve the assurance of protection from cyber threats (European Defence Fund, 2020).

The new Cyber Security Strategy also empowers the EU to enhance its leadership in establishing international norms and standards in cyberspace, as well as to bolster collaboration with global partners in advancing a global, open, stable, and secure cyberspace founded on the principles of the rule of law, human rights, fundamental freedoms, and democratic values.

Moreover, the Commission is presenting proposals to enhance the resilience of both cyber and physical infrastructure of critical entities and networks through two directives: a revised NIS Directive (or "NIS 2") aimed at ensuring a high common level of cyber security across the Union, and a new directive focusing on the resilience of critical entities. These directives span across various sectors and seek to address present and future risks, whether online or offline, including cyberattacks, criminal activities, or natural disasters, in a coherent and complementary manner. To summarise the legal and data protection environment framework for the financial sector, the main areas could be named (Table 1.7).

The European Union has taken steps to strengthen cyber security and protect critical infrastructure due to varying levels of preparedness across member states, which create vulnerabilities.

Table 1.7. Regulations and security standards framework (compiled by the author, based on Holler et al., 2020; Congressional Research Service, 2023; World Bank Group, 2020)

International Data Security Standards	
Specific to the Financial Sector	Multisectoral/General
PCI-DSS (Payment Card Industry Data Security Standard) is a regulatory framework designed to address card-related concerns and ensure the secure storage, processing, and transmission of data. While originating in the USA, its impact is global due to the widespread operations of card providers such as VISA and Mastercard across numerous countries. The standard's objective is to minimise credit card fraud and enhance the security of cardholders. Any organisation or payment service provider is obligated to adhere to this standard.	ISO 27001 is an internationally recognised data security standard that is significant within the financial sector and across various industries. Approved and released as an international standard in October 2005 by ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission), it outlines the criteria for establishing, implementing, maintaining, and enhancing an information security management system (ISMS). These standards impact financial institutions and other sectors, setting forth guidelines to ensure robust information security practices.

End of Table 1.7

International Data Security Standards	
European Regulations	
PSD2 (Payment Services Directive 2) is an EU Directive that regulates payment services and providers within the European Union (EU) and the European Economic Area (EEA). The primary goals of the PSD2 Directive include fostering a more unified European payment market, enhancing payment security, and ensuring consumer protection.	EU-GDPR, known as the General Data Protection Regulation (GDPR), is the European regulation governing the protection of individuals' data processing and the free movement of such data. This regulation applies at the European Union level, meaning that any company, including financial services entities within the Union or those conducting business in the EU and handling any form of personal information, must comply with its provisions. Non-compliance with GDPR can result in fines of up to EUR 20 million.
PSD2-RTS (PSD2 Regulatory Technical Standards), introduced at the close of 2017, encompasses a delegated regulation by the European Commission outlining the responsibilities and duties of payment intermediaries. These standards delineate precise protocols aimed at safeguarding customer communication and data. Among its mandates, PSD2-RTS necessitates the utilisation of electronic identification, authentication, and trust services (eIDAS).	The NIS Directive (Network and Information Systems Security) implements legal measures to enhance cyber security across the European Union, ensuring member states' readiness by mandating sufficient preparedness, including establishing cyber security incident response teams (CSIRT) and competent national authorities for NIS. It also encourages member states' cooperation through the creation of cooperation groups and aims to foster a culture of safety in critical sectors of the economy highly reliant on ICT, such as Energy, Transport, Water, Banking, social services, Health, and Digital Infrastructure. As part of the new European cyber security strategy, two directive proposals have been introduced to establish a standardised level of cyber security within the Union, namely "NIS2" and the Critical Entity Resilience Directive.

The 2016 Network and Information Security (NIS) Directive was established to increase cooperation and communication among EU countries, requiring them to develop national security strategies, designate cyber security authorities, and establish a framework for sharing information and responding to incidents. The NIS Directive covers critical sectors including the financial sector, mandating incident reporting and risk management measures.

The EU's broader cyber security strategy focuses on fostering resilience against cyber threats and promoting a safe digital transition. The strategy also seeks to enhance the EU's operational capabilities to effectively prevent and respond to cyber threats.

The financial sector has specific regulations like the Payment Card Industry Data Security Standard (PCI-DSS) and the Payment Services Directive 2 (PSD2), with broader guidelines provided by the General Data Protection Regulation (GDPR) and ISO 27001:2022. These initiatives aim to ensure robust cyber security practices and avoid penalties by fostering a culture of safety and compliance.

1.4. Theoretical Analysis of the Composite Index

A composite indicator or index could be described as a tool that compiles different indicators into one single index (Oslo, 2018). These indexes could combine indicators from the exact dimensions (e.g., other types of expenditure) or indicators measured in multiple or various sizes (e.g., investments indicators, innovation indicators, and framework conditions).

In comparison to simple indicators usually used in dashboards, constructing a specific composite index requires these additional steps:

1. Multiple indicators must be normalised (if they are measured using different scales, normalisation is required to put them on a single scale).
2. Data aggregation of normalised indicators into one single composite index.

Significant international organisations such as OECD, the EU, the World Economic Forum, and the IMF use composite indicators in various research and fields (Nardo et al., 2005). A general objective of most of these indicators is the ranking and benchmarking according to some aggregated dimensions (Kleinknecht, 2002). In recent years, composite indexes became typical for various uses and issues:

1. Representing some significant issues and used for advocacy matters (like measuring corruption and unemployment).
2. For monitoring general social-cultural issues (policy-making and providing analyses).

3. For tracking and monitoring processes that are in action (evaluation of the effectiveness of policies and their implementations).
4. For informational purposes (concluding institutional rankings).

These dimensions or phenomena are usually measured across several units, which may be in different countries or regions and can also be institutions or business companies. The result of constructing a composite index is usually used for comparison, ranking some units with one another.

Regarding OECD's (2008) methodology, composite indicators (or indexes) compare the performance of different countries. This tool is considered to be helpful in analysis and comparison. These indexes could help to create a simple comparison of issues in a wide range of areas that sometimes could be difficult to compare. Despite that, composite index interpretation could send a misleading message or lead to wrong conclusions if the index is poorly constructed.

In general terms, the composite index is a quantitative or a qualitative measure derived from a series of observed facts that can reveal relative positions (e.g., of a country) in a given area (OECD, 2008). If calculated and analysed regularly, a composite index could lead to a direction of necessary changes or improvements across different areas in the organisation.

According to Greco et al. (2019), with no united and meaningful possibility of being included in a common measurement, indicators could be gathered to create a composite index. The main goals of composite indexes are as follows:

1. If calculated regularly for some time, composite indexes could help evaluate changes and development.
2. Composite indexes are helpful for the visual interpretation of selected areas or phenomena.
3. Composite indexes could be analysed and used as benchmark values to monitor progress.
4. If some values could not be compared otherwise, a composite index could help as a tool for integration into one dimension.
5. Composite indexes are valuable when communicating with society or any groups of interest because they provide an easy and understandable way to evaluate and compare phenomena.

A composite index is concluded when separate indicators are compiled into a single index based on an underlying model. The composite index should ideally evaluate multidimensional concepts that a single indicator cannot capture, such as competitiveness, industrialisation, sustainability, and single market integration.

The main idea behind a composite index is to combine complex information from multiple indicators or variables into a single, comprehensive metric. This aggregated metric aims to provide a simplified yet informative summary of a broader concept or phenomenon (Table 1.8).

Table 1.8. Typology of the composite index (compiled by the author based on OECD, 2008; Oslo, 2018; Nardo et al., 2005; Kleinknecht, 2002)

Feature of the composite index	Description
Aggregation of Multiple Indicators	Composite indices combine several individual indicators or variables that collectively represent a broader concept, such as economic development, environmental sustainability, or social progress.
Simplification of Complexity	By condensing diverse information into a single numerical value, composite indices simplify the complexity of assessing multifaceted phenomena. This simplification allows for easier comparisons and communication of overall performance.
Holistic Measurement	Composite indices offer a holistic measurement of a particular aspect, considering various dimensions or components. This holistic approach captures the interplay and interactions among different factors.
Weighting and Aggregation	Indicators may contribute differently to the overall index based on relative importance. Weighting and aggregation techniques combine these indicators, reflecting their significance in the overall assessment.
Benchmarking and Comparison	Composite indices facilitate benchmarking and comparison among entities such as countries, regions, or organisations. They provide a standard metric for evaluating and ranking performance in an easily understandable way.
Public Awareness and Advocacy	Composite indices are frequently used to raise public awareness about critical issues. They can serve as advocacy tools, drawing attention to specific challenges and encouraging discussions about potential solutions.
Public Awareness and Advocacy	Composite indices are frequently used to raise public awareness about critical issues. They can serve as advocacy tools, drawing attention to specific challenges and encouraging discussions about potential solutions.
Monitoring Changes Over Time	Composite indices enable the monitoring of changes and trends over time. Regular updates to these indices provide insights into the dynamics of the measured phenomenon and help assess the impact of interventions or policy changes.
Interdisciplinary Applications	Composite indices often integrate data from various disciplines to capture the multidimensional nature of complex phenomena. This interdisciplinary approach allows for a more comprehensive understanding of the subject under investigation.

Composite indexes are like summary scores that combine many different pieces of information into one number. This makes it easier to understand complex ideas like economic issues, business development, and risk awareness. They work by giving each piece of information a score based on how important it is and then adding them all up. This helps show how different factors interact and affect each other in a holistic approach. The general pros and cons of constructing and using a composite index are described in Table 1.9.

Table 1.9. Main advantages and disadvantages of the composite index (compiled by the author based on Saisana & Tarantola, 2002; OECD, 2008)

Advantages	Disadvantage
1. Capable of condensing intricate, multifaceted realities to aid decision-makers. 2. Offer simpler interpretation compared to numerous individual indicators. 3. Able to gauge countries' advancement over time. 4. Diminish the apparent volume of indicators while retaining the fundamental information. 5. Consequently, accommodating additional information within existing size constraints becomes feasible. 6. Position issues regarding country performance and advancement as focal points in the policy sphere. 7. Enhance communication with the public (e.g., citizens, media) and foster accountability. 8. Assist in crafting/underpinning narratives for both general and educated audiences. 9. Facilitate effective comparison of intricate dimensions for users.	1. Poorly crafted or misunderstood indices could convey inaccurate policy implications. 2. There is a risk of drawing over-simplified policy conclusions from such indices. 3. If the construction process lacks transparency or solid statistical and conceptual foundations, there is potential misuse to support predetermined policies. 4. The selection of indicators and their weighting may become contentious political issues. 5. Lack of transparency in the construction process might obscure significant deficiencies in certain areas, making it challenging to identify appropriate corrective measures. 6. Neglecting dimensions of performance that are challenging to quantify could lead to the adoption of inappropriate policies.

In summary, composite indices combine complex information into a meaningful metric that facilitates comparison, decision-making, and public awareness. They are powerful tools for summarising and communicating information about multifaceted concepts in a way that is accessible and actionable.

1.5. Conclusions of the First Chapter and Formulation of the Dissertation Objectives

Summarising all the scientific literature research, the following conclusions are made:

1. Cyber security has been one of the most relevant business risks in recent years, and according to scientific research, the significance of this risk could only increase. Even though evaluating cyber risks or security levels could be rather difficult, it is significant for business continuity, reputation, and profitability.
2. Literature analyses proved that the consequences of cyber breaches are directly related to the type of cyber risk. Since various methods or suggested ways to classify cyber risks exist, the possible outcomes and damage could differ. Cyber risk classification is crucial to activating risk management, preparedness actions, and possible cost estimation.
3. In the context of cyber security, financial institutions (banks, insurance companies, credit unions, investment companies, brokerage companies, and others) are among the most important and vulnerable. As scientific literature research has proved, because of the wide range of susceptible information and data that financial institutions possess, their exposure to cyber risks is one of the highest. Generally, the concept and specifics of financial services activity make these companies highly attractive to cyber attackers.
4. Based on previously completed research and analyses of financial institutions and cyber security, it is implied that financial institutions must engage in cyber risk identification, management, and evaluation processes to ensure secure financial services and comply with a wide range of legal requirements.

Based on the conclusions, the following objectives are formulated to achieve the goal of the dissertation:

1. To establish a methodology for a tool that allows the assessment of cyber security in a financial institution.
2. Develop a unique questionnaire matrix to conduct an internal assessment of a financial institution’s cyber security level based on the provided cyber security indicators.
3. To create a tool for cyber security evaluation in financial institutions by proposing a composite cyber security index as a final result.

4. Assess cyber security in selected financial institutions to practically verify the proposed composite cyber security index.

These objectives will be further addressed in the dissertation.

2

Methodology to Construct a Tool for Cyber Security Evaluation in Financial Institutions

This chapter provides the framework of the dissertation, investigation of possible methods to evaluate cyber risks, organisational preparedness estimation methods, possible consequences measurements, methods to estimate financial impact, the framework of cyber security areas evaluations, and the methodology for the composite index construction. It also indicates multi-criteria decision-making methods usable in the context of composite index calculations. Two scientific publications were published on the topic of this chapter (Gavenaite-Sirvydiene & Miecinskiene, 2021; Gavenaite-Sirvydiene & Miecinskiene, 2023).

2.1. Process Description for the Development of a Cyber Security Evaluation Tool for Financial Institutions

The main goal of this dissertation is to establish an effective tool for financial institutions to evaluate the cyber security level, to indicate weak areas and to

understand what cyber security indicators could be improved to increase the general cyber security level and minimise the possibility of cyber risk exposure.

Generally, this tool is composed of a unique internal evaluation questionnaire that allows a financial institution to evaluate each area and indicator of cyber security separately. This internal evaluation, together with specifically identified weights of each indicator, allows for the creation of a composite cyber security index that shows the general cyber security level in that institution.

To establish this tool, the significance of cyber security was evaluated first. A few different methods were used: the Global Cost of Cyber Risk calculator was used for the financial significance aspect as it allows for the estimation of possible financial damage and confirms how crucial this issue is in financial institutions, expert interviews and the MCDM method TOPSIS were used to identify most significant cyber risks, most vulnerable organisational areas, preparedness, and other vulnerabilities related to cyber security.

Furthermore, to complete a deeper cyber security analysis in financial institutions, four significant areas were identified, and each of these areas was assigned indicators based on expert interviews and evaluations. By using the MCDM method SAW, specific weights for each indicator were calculated.

By using all the above-mentioned research results, a unique questionnaire for financial institutions was created that requires the evaluation of the internal situation in the context of each cyber security area and indicator.

Combining the specific weights of each cyber security indicator and the results from the institution's internal evaluation questionnaire, the general formula for the composite cyber security index was created, and it is the final result of the cyber security evaluation process in the financial institution (Fig. 2.1).

The process for developing a composite cyber security index consists of these main steps:

1. Evaluating most relevant cyber risks in financial institutions; general cyber security significance importance in the context of other business risks.

2. Developing the structure of main cyber security areas.

3. Identifying the most important indicators to represent each area and cover essential cyber security issues in that specific area

4. Completing research based on experts' evaluations to determine an individual weight for each of the indicators.

5. The OECD methodology and the Simple Additive Weighting method (SAW) were used to establish the final formula for the composite cyber security index.

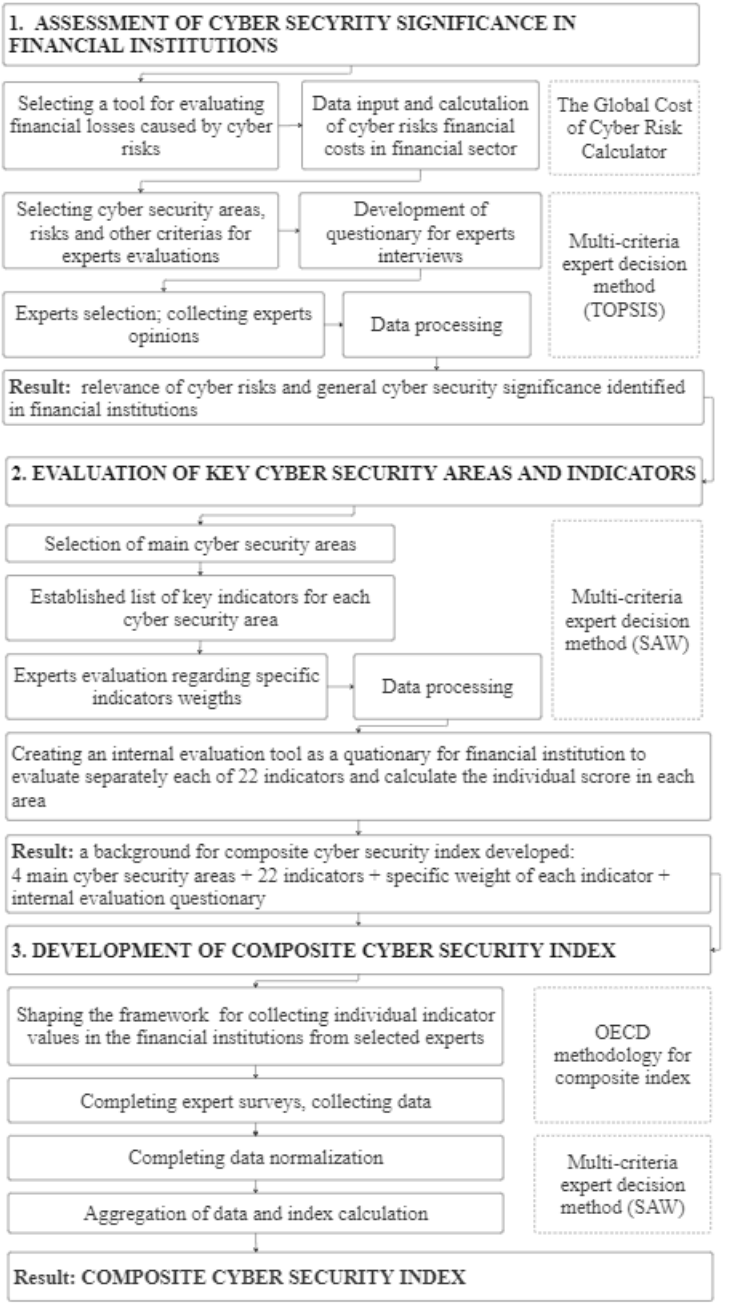


Fig. 2.1. Methodology for the development of a tool for evaluating cyber security in a financial institution (compiled by the author)

Therefore, the following research actions enabled to discover a final structure of the composite cyber security index and use it practically in financial institutions.

2.2. Evaluation of the Financial Aspect of Cyber Security in Financial Institutions

Cyber risk is a fundamental component of the overall risk faced by any organisation. Managers need to be able to quantify it to plan the level of security investment and assess the resulting risk reduction. Accordingly, they may decide to share the residual risk with a third party, such as an insurance or reinsurance company. The Global Cost of Cyber Risk Calculator, proposed by Drayer et al. (2018), can be effectively used to estimate the financial damage that a cyber security breach could cause to a financial institution. The purpose of this tool is to provide a model for assessing current and potential losses from cyber-attacks, considering the frequency, uncertainty and different types or sources of potential cyber-attacks.

The general characteristics and functions of this calculation model are as follows:

1. Determining the VaR indicator by a business line and geographical area.
2. Calculating immediate losses by including different financial situations for each business area and the proportion of each situation that may be exposed to cyber threats.
3. Calculating systemic losses from cyber-attacks across business lines using the information of the Organisation for Economic Co-operation and Development on input, output, and value-added across industries in more than 60 locations.

Cyber risk management techniques include various quantile-based measures commonly utilised within financial institutions. These measures, such as value at risk, are adapted to the cyber domain and are referred to as cyber value at risk (Cy-VaR). The concept of cyber value at risk was initially introduced by JP Morgan in 1995 (Gilli et al., 2019). This risk measure indicates, at a specified confidence level, the anticipated worst-case loss over a defined period. Leveraging the principles of VaR and aiming to assist organisations grappling with cyber security challenges, the World Economic Forum's Partnering for Cyber Resilience initiative (WEF, 2012) developed a model for assessing and quantifying the impact of cyber threats on businesses and their exposure to them. Known as cyber value-at-risk (Cy-VaR), this method serves as an initial framework for quantifying risk and instilling greater discipline in this area, albeit requiring further refinement and field testing (Buith & Spataru, 2015).

In line with the above-mentioned concerns, Cy-VaR has been increasingly incorporated into the realm of cyber security in recent years, with numerous efforts directed towards aligning this risk measure with methodologies specifically tailored for assessing cyber risk. These novel models, referred to as Cy-VaR, furnish responsible management personnel with a singular risk metric and a statistical probability, facilitating a comprehensive understanding of an enterprise's overall cyber security risk (Beckstrom, 2014). The primary objectives of Cy-VaR are twofold: to assist risk and information security professionals in articulating cyber risk in financial terms and to enable business executives to make judicious decisions that strike a balance between safeguarding the organisation and sustaining its operations (Freund & Jones, 2014).

Cy-VaR is based on the VaR concept, a risk measure proposed by JP Morgan in 1995 as the predicted worst-case loss at a specific confidence level. VaR is considered a main risk measure. Moreover, regulators state it in the Basel II and Basel III records (Gilli et al., 2019).

Organisations are accustomed to estimating VaR as part of their enterprise risk assessment, while others have applied VaR to cyber risks. Historically, these risks have been managed simply by preventing attacks or responding to them on time. However, technical reviews of security controls cannot help quantify the economic impact of cyber-attacks. Managers need to quantify cyber risks, plan the level of security investment and estimate the resulting risk reduction. They must also decide whether to share the residual risk with a third party, such as an insurance company. The rationale behind value-at-risk models applied to the cyber domain helps to address these issues. Cy-VaR allows one to explore the consequences of additional threats and compare how different configurations of security controls can help limit residual risk as the threat increases (Erola et al., 2021).

The loss distribution approach is the best-known approach to operational risk measurement and regulatory capital calculation (Locher, 2005). It is a commonly used statistical approach in the actuarial field and is based on the concept that losses can occur randomly in frequency and severity according to characteristic distributions. Specifically, the frequency and severity of losses are each assumed to independently follow a statistical distribution, with parameters estimated directly from the data (Carfora & Orlando, 2019). A closed form for such a distribution is not always achievable. Consequently, it is necessary to rely on simulation techniques to estimate its quantiles, the corresponding VaR measure, and the unexpected loss, given by the losses in between the expected loss and the value at risk (Panjer, 2006).

The cyber security literature typically models frequency by either a Poisson or negative binomial distribution (Eling & Loperfido, 2017). An appropriate way

to model the effect of mitigation on the frequency of attacks is to rely on a Poisson process (Bentley et al., 2020).

In terms of severity, log-normal and skew-normal models are commonly used in the actuarial literature. Extreme Value Theory (ETV) models are also popular because operational risk data is heavily skewed. The peaks-over-threshold (POT) method is the most common EVT approach because it is more efficient compared to other methods (Strupczewski, 2019). This approach allows modelling losses above a threshold (e.g., the 90% quantile) with a generalised Pareto distribution (GPD) and losses below the threshold with another common loss distribution. The application of these models in the cyber risk domain is suggested by Eling and Loperfido (2017). It is noted that different cyber incidents often have different statistical characteristics, which require separate modelling (Carfora et al., 2019).

Another issue is the dependency structure of losses, which requires a model that can handle different but dependent classes of losses (Bentley et al., 2020). Copulas are commonly used to model the dependence structure (Bentley et al., 2020; Eling & Jung, 2018). Recent actuarial research has focused on modelling the dependency between claim frequency and average severity (Fig. 2.2).

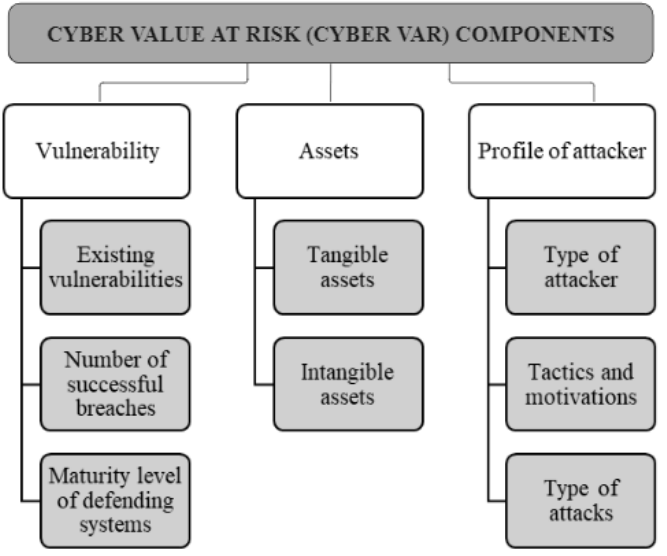


Fig. 2.2. Cyber value at risk (Cy-VaR) components
(compiled by the author based on the World Economic Forum, 2013;
Alemany et al.,2021; Bentley et al., 2020; Eling & Jung, 2018)

Cy-VaR evaluates the unforeseen loss at a designated confidence level within a specific timeframe. It aids in tackling significant concerns, such as quantifying losses stemming from cyber incidents over a defined period and gauging the

potential risk reduction for an organisation through increased security investment. While delving into these issues is complex and fraught with uncertainties, Cy-VaR can serve as an effective tool for the risk assessment process and ensuing discussions. Contrary to traditional cyber security approaches, which typically focus on the attacker's profile and attack methods, Cy-VaR examines the three fundamental components of cyber risk: vulnerability, assets, and potential attacker profiles. A well-suited Cy-VaR model should encompass the threat type executing the attack scenario, the attack types, and the system's vulnerability while also considering its maturity level. Despite the importance of these objectives, achieving them remains challenging.

Accurate estimates of Cy-VaR require accurate information about every computer vulnerability at every level of an organisation, reliable assessments of assets and business activities, and the expertise to predict the behaviour of customers, hackers, and employees. Given that perfect information does not exist, proper risk assessment and estimation are even more important, and Cy-VaR provides a reasonable approach and target to work towards.

To include possible instability in the method, the authors accepted many indicators described by attitude evaluations or possibility distributions. Outputs can be the medium values or cumulative allocations of these losses around different locations and industries.

The created model allows the evaluation of the effect of various cyber-attacks on the value-added gross domestic product (GDP) of businesses in the region. To construct this model, these criteria are necessary to be indicated (OECD, 2018):

1. Countries.
2. Industry sectors.
3. Economic exposure.
4. Perils.

A model is constructed with a dimension of countries C, industry sectors I, economic exposures E, and perils P. Thus, each country c is in the dimension of countries C, each industry sector i is in the dimension of industry sectors I, each financial exposure e is in the dimension of economic exposures E, and each peril p is in the dimension of perils P, where a cyber risk event can be followed by actions on objectives in terms of costs incurred by the defender. The dimensions are implemented as a definition and, therefore, cannot be split.

Each dimension is described in terms of the content of another but cannot be both incompatible and comprehensive. For example, the countries dimension C is a sub-dimension of all countries in the world, and its value depends on the accessibility of information. The industry dimension I is also described as incompatible or comprehensive. For example, the financial exposures dimension E and the hazards dimension P are described as both mutually exclusive and collectively exhaustive; the overarching nature of cyber-attacks may extend this

dimension beyond the current descriptions in this methodology. The authors of the model also assumed an additive separation of direct costs so that in estimating direct expenditure, sub-dimensions within each dimension do not influence each other but are linked to the broader systemic expenditure estimates (Lloyd's, 2018).

The method of investigation relates losses from cyber-attacks to GDP losses in a given sector and industry. This approach considers both rebound results between organisations (where damage in one organisation may lead to benefit in another) and reduces the need to calculate across different, largely uncertain types of damage.

Specifically, costs are divided into (OECD, 2018):

1. Output damages are handled by every sector in every country *c.*
2. The macroeconomic effects to output accepted by different sectors, therefore of the direct expenditures by every sector i in every country *c.*

In this context, direct costs pertain to expenses exclusively borne by the industry during any instance of a cyber-risk event. These costs encompass expenditures related to the implementation of safeguards, penalties, damages and investigation costs incurred, and the cessation of business activities within the affected industry following a cyber-attack. Additionally, this includes potential legal fees associated with lawsuits filed by third parties, which are covered by the organisation affected by the cyber-attack.

The general outputs of the analysed tool:

1. The total yearly losses for every region are strictly because of cyber-attacks.
2. The systemic costs for every industry regarding upstream failure caused by cyber-attacks.

This calculator model either generates the possible values of losses provided by the general results of the input data or uses the general results to assess the purpose of the losses. In this calculator, for each sector I in country C, the immediate costs of exposure and GDP are calculated by concluding the dimensions (c, i, e, and p) to G_C (the country's GDP). These steps are as follows (Dreyer et al, 2018):

1. First, w_{ci} is defined as sector i's shares of GDP in country c.
2. $w_{ci} \times G_c$ is the value added (contribution to GDP) of sector i in country c.
3. Oci is defined as the sector output of sector i in country c.
4. The unitless value Ycie is described to be the fraction of industry sector output that is adequate to the amount of money at risk from every possibility type (e), regardless of whether they can be affected by a cyber-attack.

5. The unitless value Xciep is defined as the proportion of the outcome at risk in country (c), industry (i) and exposure type (e) that is destroyed, stolen or otherwise lost due to a particular hazard (p).
6. The merger of Ycie and Xciep indicates the fractional effect of every cyber peril (p) on the exposure and/or value-added of every sector i related to every exposure e.

Based on the measurements and links provided, the direct cost of sector exposure in each sector i in country c can be determined by the sum over the product Ycie and Xciep for all perils p and outcomes e. This, multiplied by the exposure of sector i in country c (O_{ci}), gives the total direct cost of sector exposure as follows (Dreyer et al, 2018):

$$d_{cio} = o_{ci} \times Y_{cie} \times X_{ciep}. \quad (2.1)$$

Here:
d_{cio} is the total sector direct costs
o_{ic} is the sector output of sector i in country c
Y_{cie} is the fraction of industry sector output that is adequate to the amount of money at risk from every possibility type (e), regardless of whether they can be affected by a cyber-attack
X_{ciep} is the proportion of the outcome at risk in the country (c), industry (i) and exposure type (e) that is lost due to a particular hazard (p)

Considering possible modifications in sector exposure scale to changes in sector GDP, the direct exposures to sector GDP can be closely described, letting d_{cig} denote the loss to sector GDP (Dreyer et al, 2018):

$$d_{cig} = w_{ci} \times G_c \times Y_{cie} \times X_{ciep}. \quad (2.2)$$

Here:
d_{cig} is the total loss to sector GDP
w_{ic} sectors i share of GDP in country c
G_c is the country's GDP
Y_{cie} is the fraction of industry sector output that is adequate to the amount of money at risk from every possibility type (e), regardless of whether they can be affected by a cyber-attack
X_{ciep} is the proportion of the outcome at risk in the country (c), industry (i) and exposure type (e) that is lost due to a particular hazard (p)

Moreover, combining sector-level direct costs (d) allows for the evaluation of the total direct costs to exposure and GDP from cyber risks for every country c like the following (Dreyer et al, 2018):

$$d_{co} = d_{cio} \times d_{cig}. \quad (2.3)$$

Here:
d_{co} is the total direct costs to output and GDP from cyber incidents for country c
d_{cio} is the total sector direct costs
d_{cig} is the total loss to sector GDP

Due to the density of sets and the instability of cyber risk projections, it is possible to evaluate how different methodological approaches affect the well-understood value of the GDP of country C in sector I. The outcome evaluation may rely heavily on the inputs of perils, exposures, industries and their combinations. Thus, the input of sectors and exposures is simple, but the evaluation of the impact of perils on exposures is very complicated. Therefore, the method is designed to expose the uncertainty around these inputs by allowing users to change the input relationships and show the affected changes in the final calculations.

This estimation model makes it possible to update any of the dimensions or the links between the dimensions for the present or the future. For example, it is possible to:

1. Indicate a specific GDP growth for a period.
2. Use the Organisation for Economic Co-operation and Development's (OECD, 2018) financial estimation set to complete the financial estimation overviews for one year of GDP for each country.
3. Substitute predictions of how perils (p) may change financial exposures (e).

The aforementioned effects would be manifested through the approach used to assess new costs. In each scenario, the substitutes could either be directly evaluated or inferred from probability allocations, thereby influencing the distribution of potential costs. The tool allows for an overview of expenses spanning a year within a specific region, with the caveat that these general estimates may not be region-specific (Drayer, 2016).

Essentially, this tool provides standard recommendations and assumes a 1% annual GDP growth rate for high-income countries, a 6% growth rate for upper-middle-income countries, and a 7% increase for lower-middle-income countries, as per the World Bank (2016).

Model Parameters: The calculator requires the specification of various dimensions of sets to make predictions. To execute the method and validate these calculations, the dimension sets were determined based on analyses of scientific research and data investigations. These dimensions may represent either specific evaluations or probabilistic outcomes, and their combination can yield estimated values and probability distributions of exposures (Dreyer et al, 2018):

1. Country (C). Consider that "c" represents a specific country within the dimension of countries, denoted as "C". As reported by the Ponemon Institute (2019), countries and regions currently facing heightened levels of cyber-attacks include the United States, the United Kingdom, Germany, Australia, France, Brazil, Japan, Italy, India, Canada, South Africa, and the Middle East. Hence, the method should be flexible enough to accommodate potential countries facing escalating risks; thus, this dimension is expanded to encompass a broader spectrum (Anderson, 2007). Given the interconnection between countries and sectors, a wide array of data dimensions is required to encompass information on how industries relate to each country. In this regard, available data and financial information collected by the OECD are utilised.
2. Industry Sectors (I). Segmenting the economy into sectors involves employing a specific sector model based on readily available country-level data, coupled with the integration of data identified by Deloitte (2013) as pivotal for cyber risk assessment. The country-level economic data is derived from the Structural Analysis Database, with the sectors aggregated to align with Deloitte's identified significant sectors.
3. Financial Exposures (E). In this context, "e" represents the financial impact within a dimension of financial outcomes, denoted as "E", which could potentially be influenced regardless of the type of risk. These events are considered not solely in their direct correlation to GDP but as components of production susceptible to the effects of a cyber-attack, which could diminish the organisation's overall profit or revenue. This delineates the dimensions of financial outcomes as comprising capital resources, intellectual property (IP), and revenue.
4. Perils (P). Consider "p" as the risk factor within the dimension of perils, denoted as "P", where actions of cyber attackers against targets can lead to losses for the organisation. Hence, this dimension is likely to be frequently updated. This aspect is determined based on various sets of event types (Advisen, 2017). The data dimensions encompass over 12,000 cyber-attacks classified into five distinct categories for event types and 11 different categories for occurrence characteristics.

To sum up, this described calculator tool is designed to assess the impact of cyber-attacks on the GDP of a specific industry in a region. The calculator tool involves several criteria such as countries, industry sectors, economic exposures, and perils. Each dimension, like countries or industry sectors, is described in terms of content and cannot be split. The method links losses from cyber-attacks to GDP

losses in specific sectors and industries, considering both direct costs and systemic effects. The tool allows for the evaluation of total direct costs to output and GDP from cyber incidents for each country, accounting for uncertainties and allowing for modifications in inputs.

2.3. Assessment of Cyber Security Significance in Financial Institutions

Different aspects of possible and acceptable solutions are often considered – both in terms of potential costs and benefits to the organisation. Multiple-criteria Decision Analysis (MCDA) is used to select the best solution in several respects, considering the background circumstances. The TOPSIS multi-criteria expert decision analysis method was chosen as the target of this paper to assess the importance of cyber security in Lithuanian financial institutions.

Multi-criteria Analysis serves as a decision-support tool for examining alternatives to complex problems. This analytical process is characterised by its systematic, structured, transparent, and accountable nature (Opricovic, 2004). MCDA has been extensively utilised in management to evaluate decision-making options that involve balancing multiple criteria (Markovic, 2010). It can be conceptualised as an overarching term encompassing formal approaches aimed at explicitly considering multiple criteria to aid individuals or groups in exploring consequential decisions (Belton, 2002).

The MCDA process has four main components:

1. A set of alternative options.
2. A set of criteria for comparing the alternatives.
3. A weighting to assign a measure of importance to each criterion.
4. A method for ranking the alternatives according to how well they meet the criteria.

In essence, the descriptions encapsulate three key dimensions of the MCDA method: first, its formal research approach; second, its consideration of multiple criteria; and finally, its role in aiding decisions made by individuals or groups within organisations. These dimensions collectively contribute to the widespread adoption of MCDA as one of the most utilised models in business management and decision-making processes. For additional analysis, the TOPSIS method has been selected and will be employed to assess the importance of cyber security in Lithuania's financial institutions.

TOPSIS, introduced by Hwang and Yoon in 1981, is widely embraced. It operates on the principle that the chosen alternative should possess the shortest geometric distance from the positive ideal solution while maintaining the longest geometric distance from the negative ideal solution (Chakraborty, 2007;

Ginevičius, Podvezko, 2008). 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 validated instrument for handling multi-criteria decision-making (MCDM) issues, offering robust capabilities for rendering effective decisions (Velasquez, 2013). The sequence of calculations of the TOPSIS method (Table 2.1) (Simanaviciene & Petraityte, 2016).

This process allows decision-makers to evaluate and rank alternatives based on multiple criteria, considering both maximising and minimising factors to identify the most suitable option. The TOPSIS method has gained widespread popularity and recognition for its effectiveness in addressing complex decision-making scenarios across various domains. Its application extends to fields such as business, engineering, environmental management, healthcare, public policy, and more.

Table 2.1. The sequence of calculations of the TOPSIS method (compiled by the author based on Simanaviciene & Petraityte, 2016)

Step	Description
Step 1	Create an evaluation matrix X consisting of m – number of alternatives and n – number of efficiency indicators, with the intersection of each alternative and criteria given as x_{ij}; therefore, there is a matric $(x_{ij})_{m*n}$
Step 2	When applying the TOPSIS method the matrix $(x_{ij})_{m*n}$ is normalised. Normalised Decision Matrix: $$x_{ij} = \frac{x_{ij}}{\sqrt{\sum_{j=1}^{m} x_{ij}^2}} \quad (2.4)$$ Here: x_{ij} is the original value for alternative i and criterion j m is the number of alternatives
Step 3	Weighted Normalised decision matrix: $$v_{ij} = x_{ij} * q_j \quad (2.5)$$ Here: v_{ij} is the weighted normalised value for alternative I and criterion j; x_{ij} is the original value for alternative i and criterion j q_j is the value of attribute significance
Step 4	The ideal alternative and negative-ideal solutions: $A^+=(a_1^+, a_2^+, \dots, a_n^+)$ (2.6) $A^-=(a_1^-, a_2^-, \dots, a_n^-)$ (2.7) Here: A^+ is the ideal solution vector (maximising criteria); A^- is the negative ideal solution vector (minimising criteria)

End of Table 2.1

Step	Description
Step 5	The distance between the ideal A^+solution variant and comparative *i*-th is calculated by determining the distance in the n-dimensional Euclidean space using the following formula: $L_i^+ = \sqrt{\sum_{j=1}^{n} (v_{ij} - a_j^+)\,2}$ (2.8) $L_i^- = \sqrt{\sum_{j=1}^{n} (v_{ij} - a_j^-)\,2}$ (2.9) Here: L_i^+ Is the distance of alternative *i*-th to the ideal solution L_i^- Is the distance of alternative *i*-th to the negative ideal solution
Step 6	Relative Closeness to Ideal Solution: $K_i = \frac{L_i^-}{L_i^+ + L_i^-}$ (2.10) Alternatives with the highest K_i value will be considered as best alternatives.

Multi-criteria expert decision analysis (TOPSIS) was used to assess the importance of cyber security in financial institutions. To obtain valuable and reliable data, the following requirements were set for the experts:

1. Represent a financial institution (either a bank or an insurance company).
2. Have at least ten years of experience in the financial sector.
3. Hold a senior position in one of the following areas: IT security, privacy, or risk management.

The respondents were selected from six organisations, e.g., banks and non-life insurance companies operating in Lithuania. Eight experts participated in the interviews and provided their answers. The questionnaire for experts involved these general issues for measuring. Rating ranges were set from 0 to 1. The total sum of all criteria is 1 (Table 2.2).

Table 2.2. Questionnaire for experts to assess the importance of cyber security in financial institutions (compiled by the author)

Criteria	Alternatives
The most critical cyber security area in the organisation	Data security Network security Mobile security Database and infrastructure security End-user education Cloud security Disaster recovery and business continuity
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 organisation	Phishing Malware Ransomware Web application attacks Account takeover and credential abuse attacks Insider threats Denial of service
Organisation's preparedness for cyber events	Malware Insider threats 3. 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)

In summary, this TOPSIS method has such advantages as recognising the correct alternative immediately, applying it to situations with many alternatives and attributes, and is based on an aggregation function representing the "closeness to the ideal". However, there are also disadvantages, such as the lack of a means of weighting the elicitation and checking the consistency of the judgments. Also, this method needs to consider the relative importance of distances.

2.4. Framework for Evaluating Key Cyber Security Areas and Indicators

Since cyber security has been the most important risk in financial institutions for a few years, it is crucial to evaluate the key areas of cyber security. An effective risk assessment strategy and comprehensive method could be created and implemented by specifically identifying the most important cyber security areas and criteria in the financial institution.

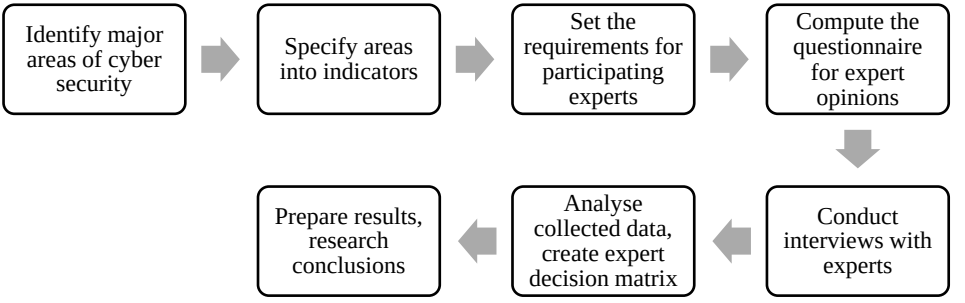


Fig. 2.3. Scheme for identifying key cyber security areas (compiled by the author)

The findings of scientific literature analyses were used to identify major cyber security areas. After segregating four major areas of cyber security that are most relevant and significant for financial institutions, a variety of indicators was selected. Different indicators were used to ensure an appropriate range of different fields and tasks were involved in this process. Each indicator (representing a specific area) led to a particular question that is dedicated to evaluating the level of awareness, preparedness, management investment, and organisational practices. Most of the questions were constructed with few possible answers, which should also represent a level of company cyber security in the particular field. In this case, the decision matrix collected from experts becomes a useful tool to identify the strengths and best practices and, most importantly, to reveal

the highest vulnerabilities, weaknesses, and areas where the cyber security lever is the lowest.

In recent years, multi-criteria methods have been increasingly used to complete the quantitative assessment of complicated economic or social issues. The general idea regarding the quantitative evaluation methods is incorporating the values of the criteria describing a particular process and their weights (significances) into a single magnitude, e.g., the criterion of the method (Podvezko, 2011). The evaluation aims to select the best alternatives by ranking the alternatives, i.e., ranking them according to their importance for the research object using quantitative multi-criteria evaluation methods. None of these methods can be used formally without prior analysis. For completing this research, multiple-criteria decision analyses (MCDA) are used to choose the solutions that could be considered the best in terms of background circumstances.

The general purpose of decision-making in economics is to evaluate and select the most preferable solution, implement it, and achieve the greatest possible gain. Preferred options are used in many problem situations in individual and organisational decision-making. In the last decade, several effective decision-making methods have appeared that support decisions under conditions of multiple criteria (Zavadskas, Turskis, 2011). Multiple-criteria decision-making (MCDM) methods provide a systematic framework for addressing decision problems involving multiple objectives, diverse criteria, and varying preferences (Sahoo et al., 2023).

The MCDM methods are considered important and valuable tools since they allow for addressing complex decision-making issues involving multiple objectives, indicators, or stakeholders (Hasan et al., 2022). These are some advantages of these methods:

1. Systematic and structured approach. Multi-criteria decision-making (MCDM) approaches offer a methodical and organised structure for the decision-making process. They empower decision-makers to dissect intricate problems into a series of criteria, assess various alternatives concerning these criteria, and make informed decisions utilising clearly defined decision rules (Li et al., 2020). This organised methodology aids in minimising ambiguity, guaranteeing transparency, and promoting uniform decision-making.
2. Multiple objectives and criteria. Numerous decisions in the real world entail the simultaneous consideration of multiple objectives. Multi-criteria decision-making (MCDM) methodologies offer a means to systematically address various objectives and criteria, allowing decision-makers to navigate and reconcile competing goals effectively (Sahoo, Goswami, 2024). These methods, by capturing the preferences and trade-offs inherent in the decision-making process, assist in

pinpointing solutions that are either optimal or satisfactory and align with the decision-maker's preferences (Gebre et al., 2021).

3. Managing uncertainty. The decision-making process frequently involves uncertainty and subjectivity. Multi-criteria decision-making (MCDM) approaches present methodologies for addressing uncertain information, employing tools like fuzzy logic or probabilistic models. This capability empowers decision-makers to formulate resilient decisions, even when confronted with incomplete or imprecise data (Pelissari et al., 2022). Furthermore, MCDM methods offer mechanisms to integrate the subjective judgments and preferences of decision-makers, ensuring that their viewpoints are appropriately reflected in the decision-making process.
4. Providing perspective of stakeholders**.** In numerous decision-making scenarios, there are multiple stakeholders with varied interests and preferences. MCDM methods enable the integration of diverse stakeholder perspectives by explicitly incorporating their criteria and preferences (Yenugula et al., 2024). This participative approach fosters fairness, inclusiveness, and stakeholder engagement, resulting in more acceptable and well-supported decisions.
5. Various applications. MCDM techniques are utilised across diverse domains such as business, engineering, environmental management, healthcare, public policy, and beyond (Supriya, Gadekallu, 2023). Whether applied in strategic planning, project selection, resource allocation, or risk assessment, these methods are valuable tools for tackling intricate decision problems in various fields. Their versatility and adaptability make them suitable for various decision-making scenarios.

Simple additive weighting (SAW) is a method used to solve multi-attribute decision questions.

The SAW method is valuable for determining the weighted performance scores for each alternative across all attributes. It effectively demonstrates the concept of consolidating the values and weights of criteria into a single estimated value – the method’s criterion. SAW necessitates the normalisation of the decision matrix (X) to a scale that permits comparison with all potential alternative ratings.

The following steps are for completing the calculation based on the SAW method (Table 2.3).

The determined weight values may be accepted and used if the expert opinions match. The compatibility of the opinions of the two experts can be quantified using the correlation coefficient.

Table 2.3. The sequence of calculations of the SAW method (compiled by the author based on Panjaitan, 2019; Ginevičius, Podvezko, 2008)

Step	Description
Step 1	Establish the criteria considered as a reference when making decisions, namely Ci.
Step 2	Determine the suitability rating of each alternative.
Step 3	Constructing a decision matrix validated on the criteria (C_i), then normalising the matrix based on the equation adjusted for the type of attribute (profit attribute or cost attribute) to create a normalised matrix R.
Step 4	The normalising matrix is based on the adapted equation with the type of benefit attribute (attribute or cost attribute) to obtain the normalised matrix R. The following formulas for completing data normalisation should be used (Panjaitan, 2019): $$r_{ij} = \frac{\min r_{ij}}{r_{ij}} \quad (2.11)$$ $$r_{ij} = \frac{\max r_{ij}}{r_{ij}} \quad (2.12)$$ where r_{ij} is the *i-th* criterion's value for the *j*-th alternative; min r_{ij} is the smallest *i*-th criterion's value for all the alternatives compared; max r_{ij} is the largest *i*-th criterion's value of all alternatives.
Step 5	The final result is obtained from the ranking process, namely, the addition and multiplication of the normalised matrix R with the weight vector so that the largest value is selected as the best alternative (Ai) solution (Panjaitan, 2019). The preference value for each alternative (V_i) is: $$S_j = \sum_{i=1}^{m} w_i r_{ij} \quad (2.13)$$ where S_j is a normalised performance rating, w_i is the weighted value of each criterion, and r_{ij} is the normalised performance rating value. The largest value of the S_j value addresses the best alternative.

If there are more than two experts, the level of compatibility of the group of experts is determined by the concordance coefficient (Ginevicius, Podvezko 2008). Kendal's concordance coefficient W is calculated according to the formula (Ginevicius, Podvezko, 2008):

$$W = \frac{12S}{m^2(n^3-n)}. \quad (2.14)$$

Where W is Kendal's concordance coefficient; S is the sum of the deviations of the ranks from the average; n is the number of objects (indicators) (i = 1, 2, ..., n); m is the number of experts (j = 1, 2, ..., m). If expert opinions practically do

not differ, the value of concordance W is close to 1, and if the assessments are contradictory, the value of W is close to 0.

Additionally, it is necessary to evaluate the reliability of expert opinions. Kendall demonstrated (Ginevičius, Podvezko, 2008) that when the number of objects (indicators) n > 7, the significance of the concordance coefficient can be determined using Pearson's criterion. The random variable identifies:

$$\chi^2 = m(n-1)W \tag{2.15}$$

distributed according to the χ^2 distribution with $\upsilon = n - 1$ degrees of freedom. Based on the chosen significance level α (typically $\alpha = 0$ or $\alpha = 0.01$), the critical value is obtained from the χ^2 distribution table with $\upsilon = n = 1$ degrees of freedom. If the calculated χ^2 value exceeds $\chi^{2\,crit}$ based on the formula above, the expert assessment is considered harmonised. The SAW (Simple Additive Weighting) method was selected as a tool to complete this research and evaluate the cyber security areas and indicators in financial institutions.

Using the multi-criteria expert decision analyses method SAW (Simple Additive Weighting), the significance of cyber security areas and weights of indicators were evaluated. To collect reliable data, these requirements for the experts were established:

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

The questionnaire for experts involved four different cyber security areas in the financial institution. These areas were selected based on the results of scientific literature analyses and data aggregation, identifying crucial aspects related to cyber security in financial institutions (Table 2.4):

1. Legal measures.
2. Organisational measures.
3. Technical measures.
4. Incident management.

Table 2.4. Questionnaire for expert evaluation regarding the significance of cyber security areas and indicators (compiled by the author)

No.	Area	Indicator
1	Legal measures	Company's internal policy/guidelines
2	Legal measures	International legal requirements (EU level)

End of Table 2.4

No.	Area	Indicator
3	Legal measures	Ensuring compliance and cyber security standards
4	Legal measures	Reports on key compliance indicators
5	Organisational measures	Cyber risk assessment and prioritisation
6	Organisational measures	Internal cyber risk controls
7	Organisational measures	Training and user education
8	Organisational measures	Investing in cyber security development
9	Organisational measures	Appointing an accountable officer (team)
10	Organisational measures	A strategic approach to cyber risk
11	Technical measures	Mapping cyber threats regarding possible loss
12	Technical measures	Specific security frameworks regarding industry standards
13	Technical measures	Third-party responsibility regarding cyber security
14	Technical measures	Identifying possible cyber-attack motivations
15	Technical measures	Access to sensitive data and internal systems
16	Incident management	Cyber risk insurance
17	Incident management	Reporting mechanism in case of the breach/cyber attack
18	Incident management	Action reviews and testing
19	Incident management	Cyber incidents response unit
20	Incident management	Cyber crisis management plan
21	Incident management	Measures and tools dedicated to reducing consequences
22	Incident management	Recovering from a cyber incident

The clustered areas were divided into a list of indicators for each area. Therefore, the experts were supposed to rank the list of indicators from the most significant to the least significant to organizations' cyber security level.

Table 2.4 outlines various cybersecurity measures, grouped into four key areas: Legal, Organizational, Technical, and Incident Management. Each area contains specific indicators that organizations should consider to ensure a comprehensive cybersecurity level:

- Legal Measures: focus on internal policies, international legal requirements, compliance with cybersecurity standards, and reports on compliance indicators.
- Organizational Measures**:** include cyber risk assessment and controls, user training and education, investment in cybersecurity, appointing accountable officers, and strategic approaches to managing cyber risks.

- Technical Measures: cover mapping cyber threats, adhering to industry-specific security frameworks, defining third-party responsibilities, identifying cyber-attack motivations, and controlling access to sensitive data.
- Incident Management: includes cyber risk insurance, reporting mechanisms for breaches, action reviews and testing, dedicated cyber incident response units, cyber crisis management plans, and tools for reducing the impact of incidents, as well as recovery strategies.

Together, these indicators provide a framework for financial institutions to establish, manage, and continuously improve their cybersecurity strategies. They address a wide range of considerations, from legal compliance to incident response and recovery.

2.5. Methodology for Establishing a Composite Index

Generally, composite indexes use a method to combine different variables into a single measure. This approach could provide a tool for analysing, measuring, and comparing subjects that could be hard to evaluate, such as social aspects, innovations, and risk preparedness. Composite indexes are often used among economic, environmental, or social areas to support the evaluation of these areas. In business, composite indexes are commonly used as a benchmark tool to evaluate progress or innovation.

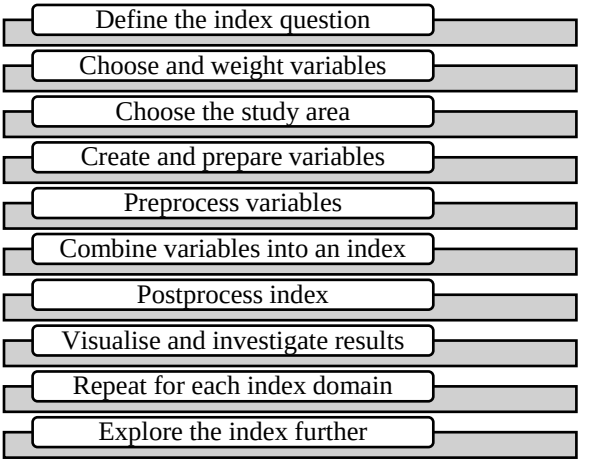


Fig. 2.4. Workflow scheme to construct a composite index (compiled by the author based on ArcGIS, 2023)

Different methodologies indicate about ten steps to develop a composite index (ArcGIS, 2023). Every step is crucial to achieve reliable results, and coherence in the process is just as important. As decisions made in one of the steps could have implications for others, following the methodology in each step and evaluating if all the steps fit together is a crucial part of index construction.

The ArcGIS document (2023) on best practices in creating composite indexes determines the following sequence of steps (Fig. 2.4):

On the other hand, OECD's (2008) methodology for composite indexes provides a slightly different sequence of steps to create the index. The table below provides the steps in the process, followed by detailed explanations of methodological tools and important notes (Table 2.5).

Table 2.5. Checklist for building a composite indicator (compiled by the author based on OECD, 2008; ArcGIS, 2023)

Steps	Why necessary
1. Theoretical framework. Provides the groundwork for selecting and merging variables into a coherent composite indicator, guided by a principle of suitability for the intended use (involvement of experts and stakeholders is envisioned during this phase).	To obtain a clear understanding and definition of the multidimensional phenomenon to be measured. Structure the different sub-groups of the phenomenon (if necessary). Compile a list of selection criteria for the underlying variables, e.g., input, output, and process.
2. Data selection. It ought to be grounded on the analytical rigour, measurability, breadth of country coverage, and relevance of the indicators to the phenomenon under assessment, as well as their interrela-tionships. When data are limited, the utilisation of proxy variables should be considered (engagement of experts and stakeholders is anticipated during this stage).	Check the quality of the available indicators. To discuss the strengths and weaknesses of each selected indicator. To prepare a summary table of data characteristics, e.g., availability (across countries and over time), source, type (hard, soft, or input, output, and process).
3. Imputation of missing data. It is needed to provide a complete set of data (e.g.,	Estimate missing values. To provide a measure of the reliability of each imputed value to assess the impact of imputation on the composite indicator results.

Continued Table 2.5

Steps	Why necessary
through single or multiple imputations).	To discuss the presence of outliers in the data set.
4. Multivariate analysis. It should be used to examine the overall structure of the dataset, assess its suitability, and guide subsequent methodological choices (e.g., weighting and aggregation).	Assess the fundamental structure of the data across the primary dimensions, encompassing individual indicators and countries, utilising appropriate multivariate methods, such as principal components analysis or cluster analysis. Identify clusters of indicators or countries demonstrating statistical "similarity" and offer an interpretation of the findings. Compare the statistically derived structure of the dataset with the theoretical framework and explore potential variances.
5. Normalisation. This should be carried out to render the variables comparable.	Choose appropriate normalisation procedure(s) that adhere to both the theoretical framework and the characteristics of the data. Address the presence of outliers in the dataset, considering their potential impact as unintended benchmarks. Implement scale adjustments if deemed necessary. Consider transforming highly skewed indicators, if required.
6. Weighting and aggregation. This should be done along the lines of the underlying theoretical framework.	Choose suitable weighting and aggregation procedure(s) that align with the theoretical framework and the data's characteristics. Consider whether correlation issues among indicators need to be considered. Evaluate whether compensability among indicators should be permitted.
7. Uncertainty and sensitivity analysis. It is necessary to evaluate the composite indicator's resilience regarding factors such as the method of including or excluding indicators, the normalisation process, handling	Consider adopting a multi-modelling approach for constructing the composite indicator and explore alternative conceptual scenarios for selecting the underlying indicators, if applicable. Identify all potential sources of uncertainty in developing the composite indicator and provide uncertainty bounds alongside the composite scores and ranks.

End of Table 2.5

Steps	Why necessary
missing data, weight selection, and the aggregation method.	Perform a sensitivity analysis on the assumptions made during inference to ascertain which sources of uncertainty exert greater influence on the scores and/or ranks.
8. Back to the data. Uncovering the primary factors influencing overall performance, whether positive or negative, is essential.	Profile the performance of countries at the indicator level to ascertain the factors influencing the composite indicator results. Examine for correlations and potential causality.
9. Links to other indicators Efforts should be undertaken to correlate the composite indicator (or its dimensions) with existing indicators, whether simple or composite and to establish connections using regression analyses.	Correlate the composite indicator with other pertinent measures, considering the sensitivity analysis findings. Craft data-driven narratives derived from the results.
10. Visualisation of the results. Given that visualisation can impact interpretability, it warrants adequate attention to ensure its effectiveness or potential enhancement.	Identify a cohesive array of presentation tools tailored to the intended audience. Choose the visualisation method that effectively conveys the most comprehensive information. Present the composite indicator results with clarity and precision.

This is a suggested ideal sequence of ten steps for developing a theoretical background and practical visualisation of the composite index. Often, the quality of the composite index depends more on a prepared and used theoretical background and the quality of the suggested framework.

2.6. Empirical Model and Structure of the Composite Cyber Security Index for Financial Institution

The cyber security index could be an efficient tool for financial institutions to evaluate their level in this field, discover vulnerable points, and identify missing opportunities to provide the business with continuous security support. Therefore, this tool's general framework and goals include various sets of practices and principles (Table 2.6).

Table 2.6. General framework for cyber security composite index in financial institutions (compiled by the author)

Area	Indicator	Weight of indicator	Scores of indicators
Legal measures	4 specific indicators	The specific weight of each indicator	Score of each indicator after internal evaluation in the company
Organisational measures	6 specific indicators		
Technical measures	5 specific indicators		
Incident management	7 specific indicators		

As already indicated in Chapter 2.4.1, the cyber security framework for financial institutions combines four major areas and is then distributed into 22 indicators. To effectively evaluate the status of cyber security, each indicator contains specific indicators that should reveal the organisation's input into cyber security issues and evaluate efforts and preparedness.

The table below shows the commitments of specific indicators per specific area covered by the indicator (Table 2.7).

Table 2.7. Main cyber security areas (compiled by the author)

Area	Explanation
Legal measures	Measuring the laws and regulations on cybercrime and cyber security. The level of the company's correspondence to legal requirements, number of legal tools and security trackers that are in use.
Organisational measures	Measuring awareness campaigns, training, education, and incentives for cyber security capacity development Also, processes, guidelines, and cyber risk identification and management strategies.
Technical measures	Measuring the implementation of technical capabilities, additional tools, investments, and other measures to prevent cyber breaches.
Incident management	Measuring a company's preparedness to manage cyber incidents, react quickly, and implement cyber risk management actions. Also, additional efforts are needed to minimise damage and recovery.

After the experts evaluated and ranked these four cyber security areas, the matrix of cyber security areas and the following indicators were created. Each

indicator represents a specific area of cyber security. Indicators are followed by specific questions and measurement scales to directly address the issues relevant to financial institutions (Table 2.8).

Table 2.8. A questionnaire matrix is used for the internal evaluation of each cyber security indicator in the financial institution (compiled by the author)

Areas	Indicators	Questions	Evaluations scores	Max Score
Legal measures	Company's internal policy/guidelines	Employee engagement in cyber security matters: – all employees in the company are introduced to cyber security guidelines – only specific employees (team leads/managers/heads) are mandatorily introduced to cyber security guidelines – only delegated people for cyber security are mandatory introduced with cyber security guidelines	(3) all employees in the company are mandatorily introduced to cyber security guidelines (2) only specific employees (team leads/managers/heads) are mandatorily introduced to cyber security guidelines (1) only delegated people for cyber security are mandatory introduced with cyber security guidelines	3
	International legal requirements (EU level)	The company follows these regulations and meets the presented requirements: – NIS Directive – GDPR – CRR and CRD IV – PSD2 – Solvency II	(5) ALL (4) 4 from 5 (3) 3 from 5 (2) 2 from 5 (1) 1 from 5	5

Continued Table 2.8

Areas	Indicators	Questions	Evaluations scores	Max Score
	Ensuring compliance and cyber security standards	Revision of the company's compliance level: – quarterly – two times a year – annually – after receiving observations from authorities	(4) quarterly (3) two times a year (2) annually (1) after receiving observations from authorities	4
	Reports on key compliance indicators	Regularity of company's reporting on legal requirements issues: – monthly – quarterly – two times a year – annually	(4) monthly (3) quarterly (2) two times a year (1) annually	4
Organisational measures	Regular cyber risk assessment and prioritisation	Risk assessment and prioritisation completed/renewed: – quarterly – every six months – annually – less than once a year	(4) quarterly (3) every six months (2) annually (1) less than once a year	4
	Internal cyber risk controls	A part of the company's turnover to cyber risk control tools/instruments: – less than 5% – from 5 to 10% – up to 10% – not investing at all	(1) less than 5% (2) from 5 to 10% (3) up to 10% (0) not investing at all	3
	Training and user education	Trainings, simulations, and lectures about cyber security organised: – monthly – quarterly – annually – not organised at all	(3) monthly (2) quarterly (1) annually (0) not organised at all	3

Continued Table 2.8

Areas	Indicators	Questions	Evaluations scores	Max Score
	Investing in cyber security development	A part of the company's turnover invested in cyber security issues and development: – less than 5% – from 5 to 10% – up to 10% – not investing at all	(1) less than 5% (2) from 5 to 10% (3) up to 10% (0) not investing at all	3
	Appointing an accountable officer (team)	Accountable team for cyber security: – one delegated person in the company – cyber security team of 2 to 5 people – cyber security team larger than 5 people	(1) one delegated person in the company (2) cyber security team of 2 to 5 people (3) cyber security team larger than 5 people	3
	Strategic approach to cyber risk	Following practises in the company: Creating cyber security strategy in the company Implementing the culture of cyber security significance Incorporate cyber-resilience governance into business strategy	(3) 3 from 3 (2) 2 from 3 (1) 1 from 3	3
Technical measures	Mapping cyber threats regarding possible loss	Estimated possible losses from cyber threats: – losses under 5% of the company's turnover – losses from 5% to 10% of company's turnover – losses higher than 10% of the company's turnover	(3) losses under 5% of the company's turnover (2) losses from 5% to 10% of the company's turnover (1) losses higher than 10% of the company's turnover	3

Continued Table 2.8

Areas	Indicators	Questions	Evaluations scores	Max Score
	Specific security frameworks regarding industry standards	Implemented industry-specific security measures: – online banking security applications – e-signature – two-sept identification requirements – other measures	(4) 4 from 4 (3) 3 from 4 (2) 2 from 4 (1) 1 from 4	4
	Third-party responsibility regarding cyber security	Cyber security responsibility for digital services providers and other outsourcing partners: – specific requirements for partners – determined partner's responsibility area – specific protection of digital services that are provided	(3) 3 from 3 (2) 2 from 3 (1) 1 from 3	3
	Identifying possible cyber-attack motivations	The company's cyber security could be violated in these areas (the scope of violations areas): – data theft – financial fraud – interrupted or damaged systems – reputational damage	(1) 4 from 4 (2) 3 from 4 (3) 2 from 4 (4) 1 from 4	4
	Access to sensitive data and internal systems	The rights to access sensitive data or internal systems are reviewed: – monthly – quarterly – two times a year – annually – no review of access rights is required	(4) monthly (3) quarterly (2) two times a year (1) annually (0) no review of access rights is required	4

End of Table 2.8

Areas	Indicators	Questions	Evaluations scores	Max Score
Incident management	Cyber risk insurance	Does the company have cyber insurance? What is the scope of coverage?	(1) YES (0) NO	1
	Reporting mechanism in case of breach/cyber attack	Guidelines for reporting, involvement at company level, and awareness of responsibilities (yes/no)	(1) YES (0) NO	1
	Action reviews and testing	Company implementing these practices: – stress testing models – possible cyber incident simulations in different levels of the organisation	(1) 1 from 2 (2) 2 from 2	2
	Cyber incidents response unit	Created a particular unit of employees to manage actions in case of a cyber attack	(1) YES (0) NO	1
	Cyber crisis management plan	Specific actions and reaction plans regarding legal, technical, and social matters	(1) YES (0) NO	1
	Measures and tools dedicated to reducing consequences	Specific tools dedicated to reducing the consequences of cyber-attacks to the technical/IT part, reputational damage	(1) YES (0) NO	1
	Recovering from a cyber incident	Company's ability to fully recover from cyber incident: – less than 30 days – from 30 to 90 days – from 90 to 180 days – more than 180 days	(4) less than 30 days (3) from 30 to 90 days (2) from 90 to 180 days (1) more than 180 days	4

The structure of this matrix represents the most important indicators that should be followed in financial institutions to ensure cyber security. Indicators are selected and involved based on theoretical research and scientific conclusions regarding specific financial institutions. The maximum score that could be achieved after completing this evaluation is 64.

Such significant indexes as the National Cyber Security Index (which compares cyber security levels in countries), the Cyber Resilience Index (which compares preparedness and resilience in countries), and the Global Cyber Security Index (which compares cyber security levels in countries) focus on the national or global levels. They help countries indicate vulnerabilities and improve cyber security at the national level, also allowing for comparison. Therefore, this new proposed index should focus specifically on financial institutions and represent areas and indicators mainly relevant to this financial area.

2.7. Conclusions of the Second Chapter

1. After research and analyses of different methods related to cyber risks or cyber security evaluation generally, the cyber security concept is a multidimensional issue involving a wide range of areas and problems; therefore, a particular method should be selected for specific research goals.
2. Especially in financial institutions, the possible costs or damage caused by cyber breaches are extremely important. A "Global Cost of Cyber Risk Calculator" is an appropriate tool to estimate possible financial damage for financial institutions. Also, this tool allows us to compare forecasted cyber risk costs in different business areas and economic sectors, together with estimations of possible growth of expected cyber risk costs in the upcoming years.
3. To evaluate cyber security in financial institutions, a structured framework of legal, organizational, technical, and incident management aspects is crucial. This framework serves to assess and rank key cyber security indicators. It relies on expert input from financial institutions to ensure a comprehensive evaluation.
4. According to the completed scientific literature research, the most appropriate methods were selected for further research and construction of a composite index: the multi-criteria decision-making methods SAW and TOPSIS to process data from expert evaluations; the OECD methodology for constructing a composite index was used for the research framework and workflow.

3

Construction of Composite Cyber Security Index for Financial Institutions

This chapter presents the results of the evaluation of cyber security significance in financial institutions. These results, together with an approximate forecast of possible losses caused by cyber risks, create a strong and significant background for establishing a composite cyber security index. After the composite cyber security index is developed, the practical approbation of the index is provided. One scientific publication was published on the topic of this chapter (Gavenaite-Sirvydiene & Miecinskiene, 2023)

3.1. Evaluation of the Possible Financial Damage Caused by Cyber Risks in Financial Institutions

Due to the variety of sensitive or personal data, financial information, and resources, financial institutions face growing pressure from cyber-attacks. Those risks come in different forms and through various channels, and in the changed business environment, they are usually harder to predict and identify. The primary

reason for the significance of cyber security in financial institutions is to secure all of the customers' data and assets. Therefore, financial institutions need to implement cyber security programs, take all possible preventive actions, and establish a plan for investments in cyber security. Moreover, the consequences of cyber-attacks, such as a leakage of personal data or financial credentials, may be critically significant for the company's reputation, financial stability, and business continuity.

To successfully assess cyber risks, and implement the required resources, and investment levels to keep the business environment safe, it is significantly important to understand the possible scope of financial damage that cyber risks could cause. This financial impact evaluation could be done by estimating the approximate costs of cyber risks. The Global Cyber Cost Calculator analysed in Chapter 2.2 was used for this task.

These are the main parameters for determining the financial impact of cyber risks:

Data Element Lists: The model uses five sets of elements: the GDP categories from the OECD data, the countries of interest, the industry sectors, the cyber perils faced, and the economic exposures to cyber perils. If a user modifies any of these elements, new table templates must be created using the Generate Table Templates and Generate Sector-Category Map buttons. These buttons will generate new tables for the user to fill on the Peril-Exposure Template, Sector-Exposure Template, and Sector-Category Map worksheets, removing all data from the sheets. The user should not modify elements of the GDP categories, as they reference the OECD data worksheets for each country.

Data Locations: for each country, the user specifies five worksheets to define the necessary parameters for the cost calculations: the OECD data worksheet (for GDP and input-output values by GDP category) and future Peril-Exposure and Sector-Exposure worksheets. The country names listed on the first column of this sheet will also appear in the drop-down menus on the output sheets. OECD data from 2011 for 62 countries regarding GDP and input-output production data by category were available. A user wanting to add a new country to the tool that does not have OECD data available should pick a similar country that does have OECD data available and use its values by proxy to generate the necessary GDP and Leontief inverse matrixes. The method for properly scaling the GDP of the new country is described in the GDP Map 2011–2016 in the section below.

Sector-Category Map: this part associates each GDP category on the OECD worksheets to an industry sector used in the model. Each OECD GDP category should be mapped to one of the industry sectors in the model by entering an X in the appropriate row.

GDP Map 2011–2016: this worksheet gives the GDP change by industry sector from 2011 to 2016 for each country and is used to map the 2011 OECD

data to 2016. If a country name does not appear on this worksheet, it is assumed that all sectors have had no GDP change from 2011 to 2016. If a new country (A) is added to the tool and the OECD data of country B are used by a proxy to represent the correct GDP for country A into the model, if GA and GB are the 2016 GDPs of the respective countries, and then if gB,I is the growth in industry sector *i* in country B from 2011 to 2016, then gA, = gB,I (1 + GA/GB) will correctly map the growth in country A that will produce the desired GDP for country A.

GDP Map Future: for each country and industry sector, this worksheet gives the projected future annual GDP change. It is used to map the values calculated for 2016 to a future year specified on the Data Element Lists worksheet. If a country name does not appear on this worksheet, it is assumed that there will be no annual GDP change in all sectors. Only point estimates of annual growth, not distributions, can be entered in this table. A country does not need to use proxy OECD data to match that country's future GDP predictions.

Peril-Exposure Template and Sector-Exposure Template: when the Generate Table Templates button on the Data Element Lists sheet is clicked, it updates both worksheets listed above. The intent is for the user then to make copies of these worksheets as needed and populate them with point estimates and/or probability distributions for analysis. The names of these new worksheets would then be added to the Data Locations sheet. The Sector-Exposure Template sheet contains the table structure to enter the amount of each sector output that is at risk for each exposure. The Peril-Exposure Template sheet contains the table structure in which to enter the effect of each peril on each financial exposure in each industry sector (as a percentage of the financial exposure). For the Peril-Exposure worksheet, the default values are assumed to apply across all sectors, but values may be entered for specific industry sectors. Entries in these worksheets may be point estimates (a number) or a probability distribution.

Outputs: this part displays overall output tables for each country:

- Present/Future Input-Output Matrix (% of Sector Output)
- Present/Future Input-Output Matrix ($M)
- Present/Future Inverse Leontief Matrix
- Present/Future Direct EV + Systemic EV Costs + GDP (by Sector).

RDM Outputs: RDM is short for Robust Decision Making; the RDM Outputs sheet attempts to show the variability of the results due to the probability distributions that populate the Peril-Exposure and Sector-Exposure sheets. This sheet estimates the cumulative distribution of costs for the specified country via multiple random draws of each distribution in the Peril-Exposure and sector-exposure sheets. In addition to a table showing the result of each set of random draws, the worksheet contains a chart that shows the cumulative distribution

function estimate for the present or future direct, systemic, and total costs, either in dollars or as a percentage of GDP.

Global Outputs: for all countries, a sector-by-sector breakdown of present or future direct, systemic, or total costs, either in dollars or as a percentage of GDP. The total across all countries in the model is also given in the last row of the table.

The cyber-attack costs were forecasted using the described *ESTIMATION, THE GLOBAL COST OF CYBER RISK CALCULATOR V 1.2* tool. The forecasted period is five years; the results are projected for 2026, and the cyber-attack costs are expressed in USD dollars.

Forecasted cyber-attack costs for these business sectors:

1. Banking.
2. Defence and aerospace.
3. Healthcare and insurance.
4. Oil, gas, and chemicals.
5. Public business and services.
6. Technology and electronics.
7. Transportation.
8. Utilities and consumer goods.
9. Retail.

First, the costs of cyber-attacks were forecasted based on the provided list of business sectors and the financial damage to each sector. The forecasted results in Lithuania were compared to the results in other Baltic states (Latvia and Estonia) (Table 3.1).

Table 3.1. Forecasted cyber-attack costs by 2026 across the industries (million, USD) (compiled by the author using Global Cost of Cyber Risk Calculator V1.2)

	Finance	Defence aerospace	Healthcare insurance	Oil, gas, chemicals	Public business, services	Technology electronics	Transport	Utilities, consumer goods	Retail	TOTAL
LTU	1.75	22.09	0.26	0.38	65.380	1.62	2.67	5.51	2.99	102.65
LV	1.06	13.27	1.15	0.65	65.998	1.527	1.672	0.89	1.91	88.127
EST	0.84	11.947	1.74	2.55	64.456	1.807	1.273	2.612	1.39	8.615

The forecast results show that the highest cyber-attack costs are predicted for public business and services sector /defence sectors. The lowest cost is estimated in the banking and technology/electronic business sectors. Generally, it is

forecasted that in five years, the costs of cyber-attacks in Lithuania will reach more than USD 102 million. Also, compared to other Baltic countries (Latvia and Estonia), Lithuania has the highest cyber-attack costs predicted in almost all industries. This could be motivated by the correlation with general county GDP, IT technology development and investment rate.

Furthermore, the percentage of cyber-attack costs from the general GDP of the sector in the county was forecasted while comparing the indicated business sectors and countries (Table 3.2).

Table 3.2. Forecasted cyber-attack costs by 2026 across the industries (% of sector GDP) (compiled by the author using Global Cost of Cyber Risk Calculator V1.2)

	Finance	Defence, aerospace	Healthcare Insurance	Oil, gas, chemicals	Public business,	Technology electronics	Transport	Utilities, consumer,	Retail	TOTAL
LTU	0.04%	0.45%	0.01%	0.01%	0.08%	0.10%	0.06%	0.11%	0.06%	0.92%
LV	0.03%	0.43%	0.00%	0.02%	0.15%	0.17%	0.05%	0.09%	0.06%	1.00%
EST	0.04%	0.51%	0.01%	0.01%	0.16%	0.14%	0.05%	0.11%	0.06%	1.09%

Based on the results of Lithuania, the national defence sector is significantly more vulnerable and exposed to cyber threats than other industries and will have higher costs from cyber-attacks compared to this sector's GDP. For instance, the financial or banking sector is one of the most attractive targets for cyber attackers, but because of the business-specific, sensitive, and private data that companies possess and use, cyber risk management is one of the top priorities in the banking sector; therefore, s possibility of cyber-attacks is under strict control. As the companies operating in this sector are still in the development stage for cyber security evaluation and management, the investments for risk controls and protection have been low, and the regulations are not as strict as for financial and government institutions, businesses are more vulnerable and exposed to cyber-attacks. Lithuania's national defence and other governmental institutions have faced cyber incidents, such as denial of services, confidential information theft, or system intrusions. The number of potential attacks is anticipated to grow because of the national significance of those institutions' activity and possessed data.

3.2. Evaluating the Importance of Cyber Security in Financial Institutions

According to the National Institute of Standards and Technology (NIST, 2022), global damages caused by cybercrime cost more than USD 6 trillion in 2022. The damage cost estimation is based on historical cybercrime figures, including recent year-over-year growth and organised crime hacking activities. This estimate was 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 organise training, self-education tools, and other measures to increase cyber security awareness. Cyber security 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 organisations, especially those tasked with safeguarding information related to national security, health, or financial records, need to take steps to protect their sensitive business and personnel information.

After completing expert interviews and collecting their opinions, all the data is processed according to the TOPSIS method.

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

First, the importance of different cyber security areas was evaluated (Table 3.3); the following results were received.

According to expert evaluation, data security was selected as the most significant field of cyber security in financial organisations as it involves not only commercial information or financial data but also sensitive and private information of customers.

Table 3.3. Most critical cyber security area in the organisation (compiled by the author)

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

Network security was selected as the second most important cyber security field because of its relevance to the company's and customer data protection and as one of the critical elements of business continuity. Also, it is essential to note that mobile security was pointed out as the third most important cyber security field in financial institutions. This issue is even more relevant since the global pandemic transferred most financial services and transactions to the online environment. Providing secure and fluent financial services using mobile applications has become one of the top priorities of financial institutions.

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 3.4).

Table 3.4. Most harmful type of cyber-attacks (compiled by the author)

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

As the experts indicate, the most harmful cyberattack is phishing, which is e-mails that appear to be from trusted sources (the bank or insurance company that the client is using) to gain sensitive information. Most likely, the attackers aim to appropriate such financial credentials as bank account details or passwords. Currently, financial institutions in Lithuania are facing increasing attacks and allocating more financial and management resources to protect their customers

from phishing attacks. The second type of cyber-attack selected by the experts is account takeover and credentials abuse. 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 organisation's activity type and implemented cyber risk management measures and other measures to prevent cyber incidents (Table 3.5).

Table 3.5. Type of cyber-attacks that is most likely to occur in the organisation (compiled by the author)

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

According to expert opinions, the results here closely correlate with the question above and indicate that the possible risks to financial institutions are phishing and malware. This indication approves the significance of safety issues related to accounts or personal credentials. Phishing attacks in financial organisations may be harmful in several 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. With the current expansion of remote work and online use of financial services, the obligation to ensure safe and fluent processes is becoming one of the top priorities for financial institutions.

The company's preparedness to identify and resolve cyber-attacks is an integral part of its cyber security environment. According to the expert's evaluations, financial institutions in Lithuania are prepared to manage malware and insider threats (Table 3.6).

This result can be explained as 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 organisation is challenging. Therefore, the most common cyber-attacks, such as account takeover and phishing, are recognised in third and fourth place in the preparedness evaluation list.

Table 3.6. Organisation's preparedness for cyber events (compiled by the author)

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

Finally, the experts evaluated the importance of cyber security and cyber risks and ranked them as the second most important type of risk (Table 3.7).

Table 3.7. Cyber risks' importance and relevance in the context of other financial and operational risks (compiled by the author)

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

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 is the most critical issue and part of business management that financial institutions focus on.

After analysing 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 sensitive and private information of customers. 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 critical for sensitive data protection, which is one of the essential elements of business continuity.

Phishing is the most significant and harmful cyber risk to the company's financial stability. 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 organisations 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. With the current expansion of remote work and online use 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 essential to identify different layers of tools that are dedicated to protecting networks and information. The attention should be focused primarily 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 significant attention to developing business resilience and preparedness levels in case of phishing or account take over risk occurs. As proved in the KOVRR(2022) report, the national defence sector is significantly more vulnerable and exposed to cyber threats than other industries and will incur higher costs from cyber-attacks. Lithuania will invest EUR 1.6 billion into developing cyber security until 2027. Continuous investments are required in the internal infrastructure, employee training, and consistent experience in identifying and solving those threats. As the attackers and their techniques evolve quickly, it is challenging to prepare an effective risk management model and fluently implement it in the organisation.

3.3. Determination of Key Cyber Security Areas, Indicators, and Weights

After interviewing experts and collecting their evaluations, steps were taken to process the data according to the SAW method (Table 3.8).

Table 3.8. List of cyber security areas and indicators for expert evaluations (compiled by the author)

Alternative	Area	Indicator	Type
A1	Legal measures	Company's internal policy/guidelines	Positive
A2	Legal measures	International legal requirements (EU level)	Positive
A3	Legal measures	Ensuring compliance and cyber security standards	Positive
A4	Legal measures	Reports on key compliance indicators	Positive
A5	Organisational measures	The cyber risk assessment and prioritisation	Positive
A6	Organisational measures	Internal cyber risk controls	Positive
A7	Organisational measures	Training and user education	Positive
A8	Organisational measures	Investing in cyber security development	Positive
A9	Organisational measures	Appointing an accountable officer (team)	Positive
A10	Organisational measures	Strategic approach to cyber risk	Positive
A11	Technical measures	Mapping cyber threats regarding possible loss	Positive
A12	Technical measures	Specific security frameworks regarding industry standards	Positive
A13	Technical measures	Third-party responsibility regarding cyber security	Positive
A14	Technical measures	Identifying possible cyber-attack motivations	Positive
A15	Technical measures	Access to sensitive data and internal systems	Positive
A16	Incident management	The cyber risk insurance	Positive
A17	Incident management	Reporting mechanism in case of breach/cyber attack	Positive
A18	Incident management	Action reviews and testing	Positive
A19	Incident management	The cyber incidents response unit	Positive
A20	Incident management	The Cyber Crisis Management Plan	Positive
A21	Incident management	Measures and tools dedicated to reducing consequences	Positive
A22	Incident management	Recovering from a cyber incident	Positive

To conduct data, the list of indicated cyber security areas and indicators was provided to experts. All the alternatives were considered positive (because of the beneficial effect of improving cyber security). The decision matrix of expert evaluations was completed, and numerical values of expert results were conducted (Table 3.9).

Table 3.9. Numerical characteristics of expert evaluation (compiled by the author)

Alternative	Average	Median	Min	Max
A1	8.88	8.0	3.0	16.0
A2	4.00	4.0	1.0	7.0
A3	6.25	5.5	1.0	15.0
A4	10.75	10.5	6.0	16.0
A5	19.63	20.0	16.0	22.0
A6	14.75	14.0	8.0	22.0
A7	17.25	17.0	12.0	22.0
A8	19.50	20.0	14.0	22.0
A9	14.50	13.5	10.0	22.0
A10	3.88	4.0	2.0	6.0
A11	14.63	15.5	8.0	21.0
A12	11.25	12.5	4.0	17.0
A13	13.25	13.0	10.0	17.0
A14	5.00	5.0	1.0	10.0
A15	6.38	6.0	4.0	9.0
A16	11.63	9.0	5.0	20.0
A17	3.00	2.5	1.0	6.0
A18	18.63	18.5	15.0	22.0
A19	10.50	10.0	7.0	15.0
A20	9.50	10.0	1.0	19.0
A21	15.63	16.5	8.0	21.0
A22	14.25	16.5	2.0	21.0

Since expert opinions and approaches to the solved problem differ, assessing the degree of compatibility of their opinions is required. The compatibility of opinions was assessed by calculating the concordance coefficient according to formula (4). The value of the calculated concordance coefficient ($W = 0.78$) showed that the expert assessments are similar, and the following calculations according to the selected method could proceed.

The steps to process the data were taken using the SAW method. Considering the general area evaluation, according to expert opinions, the most significant area of cyber security in financial institutions is organisational measures, which are very closely followed by incident and crisis management. The third place is taken by technical measures, and the fourth is legal measures. This allocation of values indicates that secure environment creation, in any case, should start with effective organisational preparedness, awareness of the issue and action plans. On the other hand, legal measures are crucial to meet legal requirements and ensure security. According to expert evaluations, operational aspects should be covered for legal measures and requirements to bring security first (Fig. 3.1).

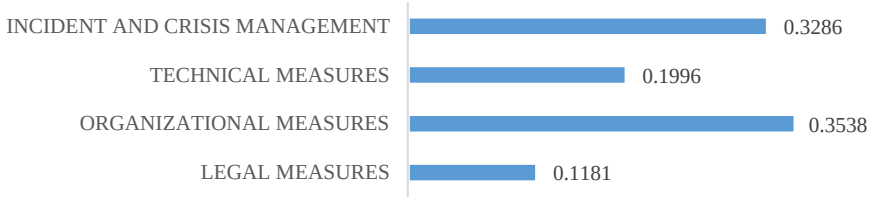


Fig. 3.1. Comparison of calculated weights of cyber security areas (compiled by the author)

Analysing indicators within the areas and starting with Legal Measures it can be stated that estimating and reporting on key compliance indicators, together with creating internal guidelines in the company, are key factors in ensuring the legal area is covered in the context of cyber security (Fig. 3.2).

Fig. 3.2. Results of indicators weights within the Legal Measures area (compiled by the author)

Variables within the "Organisational Measures" area are distributed in a wider range, prioritising such indicators as risk assessment and prioritisation, investing in cyber security development, training and user education (Fig. 3.3).

Fig. 3.3. Results of indicators weights within the Organisational Measures area (compiled by the author)

Discussing these indicators, it is important to note that risk assessment is the first step to understanding the scope of risk the company might face and leads to the next risk management steps. Investing in cyber security is one of the top priorities in the context of extremely rapid changes in the cyber security environment. Cyber-attackers improve and evolve their methods daily and analyse security and protection tools that are in the market. Therefore, not making investments and constantly developing leads to outdated tools that could easily take down cyber breaches. The third indicator is training and user education, which focuses more on a human role in this topic. Since employee awareness and understanding could be key factors in avoiding or indicating an accident, this indicator should be considered one of the top priorities.

Moving to the area of "Technical Measures" (Fig. 3.4), the most important topics to cover are probably connecting cyber risk to possible loss and estimating third-party responsibilities related to cyber issues.

First, the organisation must understand the possible scope of loss determined by a specific risk. Therefore, mapping risk to estimated costs helps the organisation prioritise correctly and allocate resources and investments to the most critical fields. Second, in financial institutions, companies commonly use a variety of services provided by third parties; therefore, it is essential to guarantee constant tracking and evaluation if the partners involved are ensuring cyber security and implementing all the necessary measures that are required.

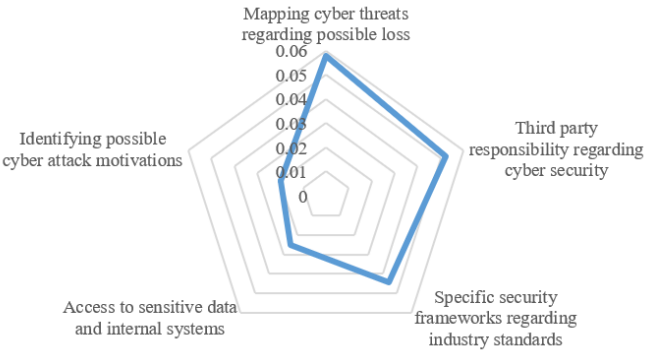


Fig. 3.4. Results of indicators weights within the Technical Measures area (compiled by the author)

The last area of cyber security analysed by experts was "Incident and crisis management" (Fig. 3.5). This area was indicated as the second most important in all scopes of cyber security issues in financial institutions.

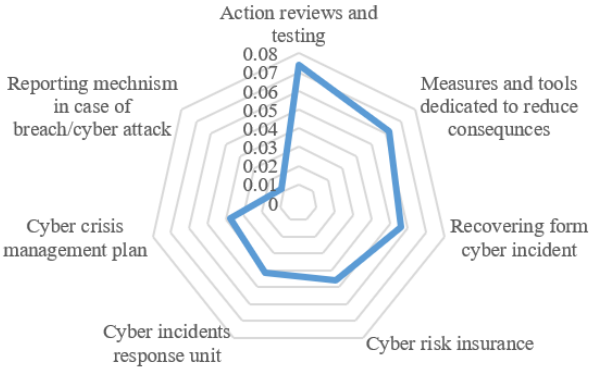


Fig. 3.5. Results of indicator weights within the Incident and Crisis Management area (compiled by the author)

In discussing incident management, the most important issue is reviewing, evaluating, and testing actions. These processes allow the company to reach a realistic view of the current situation. Reviewing and discussing actions and steps that were taken leads to changes and improvements. Also, regular testing activities not only increase awareness but also create an obligation to put efforts into understanding this field.

The final evaluations were completed after processing data and ranking values in descending order (Table 3.10).

Table 3.10. Final ranking of cyber security indicators based on expert evaluations (compiled by the author)

Area	Indicator	Alternative	Total Score (weight)	Rank
Organisational measures	Cyber risk assessment and prioritisation	A5	0.07756917	1
Organisational measures	Investing in cyber security development	A8	0.0770751	2
Incident management	Action reviews and testing	A18	0.0736166	3
Organisational measures	Training and user education	A7	0.06818182	4
Incident management	Measures and tools dedicated to reducing consequences	A21	0.06175889	5
Organisational measures	Internal cyber risk controls	A6	0.0583004	6
Technical measures	Mapping cyber threats regarding possible loss	A11	0.05780632	7
Organisational measures	Appointing an accountable officer (team)	A9	0.05731225	8
Incident management	Recovering from a cyber incident	A22	0.05632411	9
Technical measures	Third-party responsibility regarding cyber security	A13	0.05237154	10
Incident management	Cyber risk insurance	A16	0.04594862	11
Technical measures	Specific security frameworks regarding industry standards	A12	0.0444664	12
Legal measures	Reports on key compliance indicators	A4	0.04249012	13
Incident management	Cyber incidents response unit	A19	0.04150198	14
Incident management	Cyber crisis management plan	A20	0.03754941	15

End of Table 3.10

Area	Indicator	Alternative	Total Score (weight)	Rank
Legal measures	Company's internal policy/guidelines	A1	0.03507905	16
Technical measures	Access to sensitive data and internal systems	A15	0.02519763	17
Legal measures	Ensuring compliance and cyber security standards	A3	0.02470356	18
Technical measures	Identifying possible cyber-attack motivations	A14	0.01976285	19
Legal measures	International legal requirements (EU level)	A2	0.01581028	20
Organisational measures	Strategic approach to cyber risk	A10	0.01531621	21
Incident management	Reporting mechanism in case of breach/cyber attack	A17	0.01185771	22

Expert opinions and research results show that cyber risk assessment and prioritisation are the most critical financial security factors. These actions lead to a better comprehension of relevant risks in the company. Since financial institutions are a crucial target for cybercriminals, the range of possible cyber-attacks is significantly broad. As Al-Bassam (2019) indicated, financial institutions strongly depend on IT solutions and daily online operations, leading to vulnerability to cyber-attacks. Therefore, to improve cyber security levels and minimise the possibility of cyber-attacks, risk prioritisation becomes a crucial action. Moreover, the consequences of different cyber-attacks affect various fields in the company. It can cause damage to IT infrastructure, financial losses, business continuity disruption, and reputational value loss.

According to the experts, investments in cyber security are the second most crucial cyber security indicator. Especially nowadays, when the global world is at the top speed of developing technologies, artificial intelligence, and other modern IT solutions, cyber-criminals are developing fast as well. Types of cyber-attacks, malicious codes, or phishing attacks are evolving daily to adjust to the fast-changing business environment and IT security solutions. The statistical data collected by Metinko (2022) proves that global investments in cyber security significantly

increase yearly and will reach almost USD 800 billion in 2022. Therefore, financial institutions should continuously invest in cyber security training to create a safe business environment and new tools for avoiding and managing cyber-attacks.

The third and fourth indicators are closely related together. The third is action review and testing, and the fourth is training and user education. This result indicates the importance of human factors in cyber security issues. As the recent research of Georgiadou (2022) proved, a separate dimension of cyber security could be indicated for individual factors, such as attitude, awareness, behaviour, and competency. A close review of employee actions when facing cyber security issues is necessary to improve all these criteria. Reviewing the process and measures for cyber risk management can significantly improve resilience and cyber awareness in the company. Moreover, testing and simulations for employees are among the most effective tools to increase awareness and knowledge about cyber-attacks and necessary actions. It also helps to indicate vulnerable places and pain points in the cyber security process.

To conclude, cyber security issues have become a top priority in financial institutions. In the context of IT development and high dependency on online solutions, financial institutions must evaluate their cyber security environment, vulnerabilities, and resilience to cyber-attacks. To effectively create a safe business area, it is crucial to evaluate the most critical cyber security areas and indicate the most significant issues the company should focus on. As the research results implicate, the most important areas of cyber security are risk assessment and prioritisation, investments in cyber security development, action review and testing, training, and user education.

3.4. Construction of the Composite Cyber Security Index for Financial Institutions

This chapter describes the process and result of constructing the composite cyber security index for financial institutions. These results are based on the methodology provided in Chapter 2.2.2.

The first step is shaping the framework and conditions for collecting indicator values in the financial institution from selected experts. The data are coherent with the weights of each indicator and allow for further calculations.

The second step is expert surveys, data collection, and data normalisation. To make indicators comparable, values are normalised into a range between zero and one.

The last step in this process is the aggregation of data. In this phase, the composite index, which is specifically called the composite cyber security index (CCSI), is conducted. One of the most commonly used methods for conducting

composite index is Simple Additive Weighting – SAW). According to the OECD (2008), the standard practice of composite indicator creation is named a weighted linear aggregation rule applied to the range of values/indicators.

Table 3.11. Final ranking of cyber security indicators used in CCSI formula (compiled by the author)

Indicator	Weight
Cyber risk assessment and prioritisation	0.07756917
Investing in cyber security development	0.0770751
Action reviews and testing	0.0736166
Training and user education	0.06818182
Measures and tools dedicated to reducing consequences	0.06175889
Internal cyber risk controls	0.0583004
Mapping cyber threats regarding possible loss	0.05780632
Appointing an accountable officer (team)	0.05731225
Recovering from a cyber incident	0.05632411
Third-party responsibility regarding cyber security	0.05237154
Cyber risk insurance	0.04594862
Specific security frameworks regarding industry standards	0.0444664
Reports on key compliance indicators	0.04249012
Cyber incidents response unit	0.04150198
Cyber crisis management plan	0.03754941
Company's internal policy/guidelines	0.03507905
Access to sensitive data and internal systems	0.02519763
Ensuring compliance and cyber security standards	0.02470356
Identifying possible cyber-attack motivations	0.01976285
International legal requirements (EU level)	0.01581028
Strategic approach to cyber risk	0.01531621
Reporting mechanism in case of breach/cyber attack	0.01185771

Therefore, the composite cyber security index (CCSI) is calculated based on this formula:

$$CCSI = \sum_{i=1}^{n} w_i I_{Ni}, \tag{3.1}$$

here: CCSI – a composite cyber security index; w_i – a weight attached to indicator I; I_{Ni} – a normalised value of the I indicator.

The composite indicator value usually is between zero and one ($0 \leq CICS \leq 1$). The higher the value, the higher the considered level of cyber security in the organisation.

The weights used in this formula are detailed and analysed in Chapter 3.3. and connected with each indicator (Table 3.11).

Here is the completed formula for calculations of the composite cyber security index in financial institutions:

$$\mathbf{CCSI} = 0{,}035\ I_1 + 0{,}016\ I_2 + 0{,}025\ I_3 + 0{,}042\ I_4 + 0{,}078\ I_5 + 0{,}058\ I_6 + 0{,}068\ I_7 + 0{,}077\ I_8 + 0{,}057\ I_9 + 0{,}015\ I_{10} + 0{,}058\ I_{11} + 0{,}044\ I_{12} + 0{,}052\ I_{13} + 0{,}020\ I_{14} + 0{,}025\ I_{15} + 0{,}046\ I_{16} + 0{,}012\ I_{17} + 0{,}074\ I_{18} + 0{,}042\ I_{19} + 0{,}038\ I_{20} + 0{,}062\ I_{21} + 0{,}056\ I_{22} \quad (3.2)$$

This proposed composite index can be considered a comprehensive tool for cyber security evaluation in financial institutions due to the fact that it consists of four major areas of cyber security, 22 indicators within these major areas to cover the most significant issues and situations, specific weights developed based on expert evaluation and an internal evaluation questionnaire for financial institutions to calculate individual results regard each indicator. Completing an internal evaluation is a crucial part of this evaluation tool because it requires involvement from a different department in the organisation, representing not only the IT part but also a human resource, strategy implementation, and project management. Calculating scores for each indicator allows the institution to carefully research its cyber security and cyber risk management practices. The structure of the questionnaire also leads to possible improvements as the best practices are described within it.

By using this evaluation tool, financial institutions could cover and assess the relevant internal situations, discover the indicators with the lowest scores to be their significant vulnerabilities, initiate some process or investment changes regarding evaluation results, and, in this case, increase the cyber security level. Unlike other indexes of cyber risk measurement tools, this tool is exceptional in focusing specifically on financial institutions. Since the theoretical background of the tool involves such features as sensitive financial data and relevant legal regulations for financial institutions, this brings a scientific novelty and higher practical value. Moreover, selected experts who only represent financial institutions evaluated all the indicators that describe cyber security areas. Therefore, the evaluation and rankings of indicators specifically reflect the environment and issues of financial institutions.

3.5. Practical Approbation of the Composite Cyber Security Index in Financial Institutions

As already identified, the correct framework and background of the used material are essential for the following steps. Based on literature analyses (Johson, 2013; Stubley, 2013; Barzilay, 2013; Jitendra, 2017; Walls, 2013; Chapelle, 2018; Wu, 2015; Fette et al., 2007; ISO 3100:2018 standard; Strohmier et al., 2022; ENISA, 2021), the list of four areas which are represented in detail by 22 indicators, was created. Experts evaluated all the indicators by conducting a multi-criteria expert evaluation. After every indicator was assigned the weight, the following step of conducting the data regarding indicators from selected financial institutions was initiated.

As described in Chapter 2.3.2, in the questionnaire matrix for the cyber security index, three financial institutions located in Lithuania, Latvia, and Estonia were approached to collect information following the suggested matrix and conclude the cyber security index for each of the companies. In the following text, the financial institutions will be listed as LTU1, LV2, and EST3.

Considering the content of the questionnaire and the indicators involved, experts from different areas were invited to provide the answers depending on the indicator. Additional requirements for experts were also determined. First, an expert should have worked in the financial sector for no less than ten years and no less than three years in their particular company. Second, the expert should have a position no lower than the head of the division or department.

List of experts who participated in the research:

1. Data Protection Officer
2. Risk Manager/Internal Risk Manager
3. Head of IT
4. Human Resources
5. PMO (Project Management Officer)

The tables below present each financial institution's collected scores (regarding the matrix questionnaire) (Table 3.12).

Table 3.12. Indicator scores of financial institutions LTU1, LV2, EST 3 (compiled by the author)

Indicators	Code	Weight	LTU1 I_i	LV2 I_i	EST3 I_i
Company's internal policy/guidelines	I_1	0.0351	3	3	3

Continued Table 3.12

Indicators	Code	Weight	LTU1 I_i	LV2 I_i	EST3 I_i
International legal requirements (EU level)	I_2	0.0158	5	5	5
Ensuring compliance and cyber security standards	I_3	0.0247	4	3	4
Reports on key compliance indicators	I_4	0.0425	3	1	1
Regular cyber risk assessment and prioritisation	I_5	0.0776	2	2	2
Internal cyber risk controls	I_6	0.0583	1	1	1
Training and user education	I_7	0.0682	2	1	2
Investing in cyber security development	I_8	0.0771	2	1	1
Appointing an accountable officer (team)	I_9	0.0573	2	1	2
Strategic approach to cyber risk	I_{10}	0.0153	3	2	2
Mapping cyber threats regarding possible loss	I_{11}	0.0578	2	2	2
Specific security frameworks regarding industry standards	I_{12}	0.0445	3	2	2
Third-party responsibility regarding cyber security	I_{13}	0.0524	3	3	3
Identifying possible cyber-attack motivations	I_{14}	0.0198	1	1	1
Access to sensitive data and internal systems	I_{15}	0.0252	4	2	2
Cyber risk insurance	I_{16}	0.0459	0	0	0

End of Table 3.12

Indicators	Code	Weight	LTU1 I_i	LV2 I_i	EST3 I_i
Reporting mechanism in case of breach/cyber attack	I_{17}	0.0119	1	1	1
Action reviews and testing	I_{18}	0.0736	2	2	2
Cyber incidents response unit	I_{19}	0.0415	1	1	1
Cyber crisis management plan	I_{20}	0.0375	1	1	1
Measures and tools dedicated to reducing consequences	I_{21}	0.0618	1	1	1
Recovering from a cyber incident	I_{22}	0.0563	3	2	2

The next step, according to the accepted methodology, is to complete the normalisation of collected values. The following table presents the normalised indicator values (Table 3.13).

Table 3.13. Normalised indicator values LTU1, LV2, EST 3 (compiled by the author)

Indicators	Code	LTU1 normalised values	LV2 normalised values	EST3 normalised values
Company's internal policy/guidelines	I_1	0.6	0.6	0.6
International legal requirements (EU level)	I_2	1	1	1
Ensuring compliance and cyber security standards	I_3	0.8	0.6	0.8
Reports on key compliance indicators	I_4	0.6	0.2	0.2
Regular cyber risk assessment and prioritisation	I_5	0.4	0.4	0.4
Internal cyber risk controls	I_6	0.2	0.2	0.2

End of Table 3.13

Indicators	Code	LTU1 normalised values	LV2 normalised values	EST3 normalised values
Training and user education	I_7	0.4	0.2	0.4
Investing in cyber security development	I_8	0.4	0.2	0.2
Appointing an accountable officer (team)	I_9	0.4	0.2	0.4
Strategic approach to cyber risk	I_{10}	0.6	0.4	0.4
Mapping cyber threats regarding possible loss	I_{11}	0.4	0.4	0.4
Specific security frameworks regarding industry standards	I_{12}	0.6	0.4	0.4
Third-party responsibility regarding cyber security	I_{13}	0.6	0.6	0.6
Identifying possible cyber-attack motivations	I_{14}	0.2	0.2	0.2
Access to sensitive data and internal systems	I_{15}	0.8	0.4	0.4
Cyber risk insurance	I_{16}	0	0	0
Reporting mechanism in case of breach/cyber attack	I_{17}	0.2	0.2	0.2
Action reviews and testing	I_{18}	0.4	0.4	0.4
Cyber incidents response unit	I_{19}	0.2	0.2	0.2
Cyber crisis management plan	I_{20}	0.2	0.2	0.2
Measures and tools dedicated to reducing consequences	I_{21}	0.2	0.2	0.2
Recovering from a cyber incident	I_{22}	0.6	0.4	0.4

As already covered in the methodology in Chapter 2.2.2, all indicator scores are normalised between values of zero and one. Since normalisation is required before any data aggregation, for further calculations of the index, the normalised data is used. This ensures that the exact measurement units are applied to the aggregation process.

Also, the results of the three financial institutions could be compared among each other, the most sensitive areas identified, and the highest vulnerabilities in cyber security determined.

Calculated cyber security index results in three institutions (Table 3.14).

Table 3.14. Composite cyber security index in financial institutions (compiled by the author)

Financial institution	Cyber security index	Rank
LTU1	0.41413	1
LV2	0.31838	3
EST3	0.34842	2

After completing the final calculations of the cyber security index in three specific financial institutions, assumptions and evaluation of results are provided.

Analysing the results by country, it is clear that the cyber security level in all institutions is below the middle level. Institution LTU1 has the highest value, and institution LV2 has the lowest.

Going into deeper details, it is essential to pay attention to indicator weights and scores that were reached. The most important indicator of cyber security, “regular risk assessment and prioritisation”, was selected. All three companies in this area only reached half of the score (2 from 4), which means that companies review their risk assessment documentation and prioritise them only every year. In the context of a rapidly changing business and security environment, this frequency should not be considered frequent enough.

When discussing the investments in cyber security (which was also among the top five indicators selected by experts), none of the three companies reached high values. This means that companies only invest less than 5% of their turnover in cyber security development issues. Compared to the USA business environment or even some EU countries, this investment ratio is low, considering that cyber risk is among the most relevant for businesses like banks, insurance, and credit unions.

Among the most important indicators, “action review and testing” was selected. All three companies reached maximum scores in this section, which implies that companies constantly test systems and employees and evaluate their actions and knowledge regarding cyber security.

One of the key functions and use possibilities of a *composite cyber security index* is to identify vulnerabilities and weaknesses in the institution. Based on expert selections of indicators and their weights together with responses indicated by representatives of companies, the weak points deploy accordingly in the selected institutions.

Three indicators regarding expert evaluations belong to the top ten indicators and assemble the lowest scores in the company's LTU1 survey (Table 3.15).

Table 3.15. Selected major vulnerabilities regarding CCSI in financial institution LTU1 (compiled by the author)

Area	Indicator ($I_{i)}$	Alternative Rank	Normalised score value
Organisational Measures	Investing in cyber security development	2	0.2
Incident and Crisis Management	Measures and tools dedicated to reducing consequences	5	0.2
Organisational Measures	Internal cyber risk controls	6	0.2

In LTU1 financial institution, indicators with the highest ranks and lowest scores are investing in cyber security, measures and tools dedicated to reducing consequences, and internal cyber risk controls.

For LV2, financial institution indicators with the highest ranks and lowest scores invest in cyber security, training and user education, measures and tools dedicated to reducing consequences (Table 3.16).

Table 3.16. Selected major vulnerabilities regarding CCSI in financial institution LV2 (compiled by the author)

Area	Indicator ($I_{i)}$	Alternative Rank	Normalised score value
Organisational Measures	Investing in cyber security development	2	0.2
Incident and Crisis Management	Training and user education	4	0.2
Organisational Measures	Measures and tools dedicated to reducing consequences	5	0.2

For EST3, financial institution indicators with the highest ranks and lowest scores are investing in cyber security, measures and tools dedicated to reducing consequences, and internal cyber risk controls (Table 3.17).

Table 3.17. Selected major vulnerabilities regarding CCSI in financial institution EST3 (compiled by the author)

Area	Indicator ($I_{i)}$	Alternative Rank	Normalised score value
Organisational Measures	Investing in cyber security development	2	0.2
Incident and Crisis Management	Measures and tools dedicated to reducing consequences	5	0.2
Organisational Measures	Internal cyber risk controls	6	0.2

To sum up, all three companies have common weaknesses in the area of cyber security. Also, none of the companies received any scores in the area of cyber insurance (indicator I_{16}), which means there is no common practice for buying cyber insurance. Several arguments could explain this. First, cyber insurance is still a complex issue regarding evaluating risk, and the price is usually rather high. Secondly, it is not so easy to find a solution because, in Lithuania or the Baltics, there are no local products; therefore, to find a solution for cyber risk, insurance companies should search for outsourced partners.

3.6. Conclusions of the Third Chapter

1. Data security is identified as the highest priority risk in financial institutions, as highlighted by experts using the multi-criteria decision-making analysis method (TOPSIS). The significance of data security is attributed to its involvement in protecting commercial and financial data and sensitive and private customer information. The research emphasises the increasing importance of data security, with financial institutions allocating more resources and budgets to prevent sensitive data breaches. This aligns with the broader trend in the industry, indicating a growing focus on safeguarding data to mitigate potential risks and consequences.
2. The forecasted cyber-attack costs across various industries in Lithuania indicate a substantial financial impact, with predictions exceeding USD 102 million by 2026. The public business and services sector and the defence sector are expected to incur the highest costs. Compared to other Baltic countries (Latvia and Estonia), Lithuania has the highest predicted costs in most industries. The forecast also reveals that the national defence sector is particularly vulnerable and exposed to cyber threats, facing higher costs than its GDP. This vulnerability is attributed to the significant

national importance of defence institutions, making them attractive targets for cyber attackers.

3. According to expert evaluations, the most significant area of cybersecurity in financial institutions is organisational measures. This includes cyber risk assessment and prioritisation, internal cyber risk controls, training, user education, and investing in cyber security development. The text suggests that creating a secure environment should start with effective organisational preparedness and action plans.
4. Despite the importance of cyber security, the text highlights that all three financial institutions (LTU1, LV2, EST3) did not score high in the indicator "Investing in cyber security development". The low scores indicate that these companies invest less than 5% of their turnover in cybersecurity development, which is considered low, especially in the context of the rapidly evolving cybersecurity landscape.

3.7. Limitations and Future Research Directions

The following limitations apply to the conducted research:

1. The study focuses on financial institutions in specific Baltic countries (Lithuania, Latvia, and Estonia). The findings might not be universally applicable, and the cybersecurity landscape can vary significantly in different regions and types of financial institutions.
2. The study captures a snapshot of cyber security practices at a specific point in time. The dynamic and evolving nature of cyber security threats means that the effectiveness of measures may change over time, making the findings necessary for updating and renewing some details.
3. The study focuses on a specific set of indicators, and some critical aspects of cyber security may not be adequately covered. For example, the absence of a comprehensive exploration of emerging technologies, like artificial intelligence in cyber security, could limit the study's scope.

The possible directions for future work:

1. Conducting longitudinal studies over an extended period could provide insights into the effectiveness of cyber security measures over time. This would help in understanding the evolution of threats and the adaptability of security measures.
2. Expanding the research to include various industries beyond financial institutions would enable researchers to compare cybersecurity practices across sectors. This comparative analysis could highlight industry-specific challenges and best practices.

3. Extending the study to include a more diverse set of countries and regions would contribute to a more comprehensive understanding of global cybersecurity practices. This could reveal regional variations and highlight common challenges faced by organisations worldwide.
4. Future research could investigate incident response mechanisms, analysing how organisations handle and recover from cyber security incidents. Understanding the effectiveness of incident response plans is crucial for enhancing overall cyber security resilience.
5. Addressing these limitations and exploring these future research directions would contribute to a more detailed and comprehensive understanding of cyber security practices in financial institutions.

General Conclusions

1. The literature analysis highlights the increasing importance of cyber security as a significant business risk, with potential implications for business continuity, reputation, and profitability. Evaluating cyber risks and security levels is challenging but essential. Literature reviews demonstrate that the impact of cyber breaches varies depending on the type of cyber risk involved. Given the diversity of methods for classifying cyber risks, understanding these classifications is crucial for activating risk assessment strategies and preparedness measures and estimating potential costs associated with cyber incidents.
2. Financial institutions are recognised as critical and highly vulnerable entities in the realm of cyber security, primarily due to the extensive and sensitive data they handle. Scientific literature underlines the elevated exposure of financial institutions to cyber risks, given the breadth of information they manage. The nature of financial services inherently makes these organisations prime targets for cyber attackers. Previous scientific studies suggest that in order to maintain secure financial services and comply with legal regulations, financial institutions must actively engage in cyber risk assessment processes.

3. A comprehensive analysis of the components, structure and features of cyber risks and cyber security has led to the identification of four main areas of cyber security in financial institutions: legal measures, organisational measures, technical measures and incident and crisis management. Through expert interviews and MCDM methods, 22 cyber security indicators were identified (four indicators for the legal area, six indicators for the organisational area, five indicators for the technical area, and seven indicators for the incident management domain.
4. A methodology has been developed to create a cyber security assessment tool, which includes four main cyber security areas; 22 indicators; individual weights identified by experts for each of the indicators, expressing their importance in the overall cyber security context; a questionnaire for internal evaluation of each indicator in the financial institution.
5. Based on the completed scientific research, the most appropriate methods were selected for further research and construction of a composite index: multi-criteria decision-making methods (SAW and TOPSIS) to process data from expert evaluations; the OECD methodology for constructing the composite index was used.
6. Data security was identified as the highest priority risk in financial institutions, as highlighted by experts using the multi-criteria decision-making analysis method, TOPSIS. Data security is significant because it protects commercial and financial data and sensitive and private customer information.
7. Cyber security indicators were ranked after completing the expert interviews and processing results using the multi-criteria decision-making analysis method SAW. The most important indicator was selected cyber risk assessment and prioritisation, the second one – investing in cyber security development, and the third one – action reviews and testing.
8. A composite cyber security index has been developed that allows a financial institution to determine its overall level of cyber security through an internal assessment and identify problem areas. The composite cyber security index allows a detailed analysis of the areas of cyber security weakness and also allows the identification of the measures that can be taken to improve the level of cyber security.
9. The composite cyber security index has been practically applied to individually assess the cyber security level of three different financial institutions. This practical assessment allows testing the developed tool

and comparing the results between different institutions. The tool can, therefore, be used not only as an internal assessment tool but also as an overall indicator for comparing and assessing the level of cyber security in the financial sector.

References

Abdullah, A. (2019, April 29). An Overview of Risk Management Principles. *Society of Certified Risk Professionals*. https://www.scrp.org.my/

Abdullayeva, F. (2023). Cyber resilience and cyber security issues of intelligent cloud computing systems. *Results Control Optim*, *12*, 100268. https://doi.org/10.1016/j.rico.2023.100268

Advisen (2010). *Data Security Issues Escalate as Risk Management Evolves.* https://www.advisenltd.com/wp-content/uploads/DataSecurity.pdf

Advisen (2018, January 2). *Cyber Loss Dataset.* https://www.advisenltd.com/data/cyber-loss-data/

Agarwal, K., & Dubey, S. K. (2014). Network Security: Attacks and Defense. *International Journal of Advance Foundation and Research in Science & Engineering (IJAFRSE)*, *1*(3, 2339-2345. https://www.ijamtes.org/gallery/290-nov.pdf).

Al-Matari, O., Helal, I., Mazen, S., & Elhennawy, S. (2021). Adopting the security maturity model to the organizations' capability model. *Egyptian Informatics Journal*, *22*(2), 193–199. https://doi.org/10.1016/j.eij.2020.08.001

Albertazzi, U., & Gambacorta, L. (2006). Bank profitability and the business cycle. *Journal of Law and Economics*, 601, 11–18. https://doi.org/10.2139/ssrn.935026

Aliyu, A., Maglaras, L., He, Y., Yevseyeva, I., Boiten, E., Cook, A., & Janicke, H. (2020). A holistic cybersecurity maturity assessment framework for higher education

institutions in the United Kingdom. *Appl Sci*, *10*(10), 3660. https://doi.org/10.3390/app10103660 Allianz Global Corporate & Specialty. (2021, February 10). *Allianz Risk Barometer 2021: Top Business Risks for 2021* [Report]. https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html

Allianz Global Corporate. (2019). *A Guide to Cyber Risk – Managing the Impact of Increasing Interconnectivity.* https://commercial.allianz.com/news-and-insights/reports/a-guide-to-cyber-risk.html

Alsaroso, I., Frost, J., Gambacorta, L., & Whyte, D. (2020). Covid-19 and cyber risk in the financial sector. *BIS Bulletin*, 37, 3–9. https://www.bis.org/publ/bisbull37.htm

America's Cyber Defence Agency. (2022). *Guide to Getting Started with a Cybersecurity Risk Assessment.* https://www.cisa.gov/sites/default/files/2024-01/22_1201_safecom_guide_to_cybersecurity_risk_assessment_508.pdf

Anderson, R., & Moore, T. (2007). Information security economics–and beyond. In Annual international cryptology conference (pp. 68-91). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-74143-5_5

Apruzzese, G., Laskov, P., Montes de Oca, E., Mallouli, W., Brdalo Rapa, L., Vasileios Grammatopoulos, A., & Di Franco, F. (2023). The Role of Machine Learning in Cybersecurity. *Digital Threats: Research and Practice*, *4*(1), 1–38. https://doi.org/10.1145/3545574

Assaf A. (2005). Automation, Stock Market Volatility and Risk-Return Relationship. *Investment Management and Financial Innovations: Evidence from CATS*, *2*(3), 136–145. https://www.researchgate.net/publication/265922267

Baral, K. (2005). Health Check-up of Commercial Banks in the Framework of CAMEL: A Case Study of Joint Venture Banks in Nepal. *The Journal of Nepalese Business Studies*, *2*(1), 5–6. https://doi.org/10.3126/jnbs.v2i1.55

Basel Committee on Banking Supervision. (2018). *Cyber-resilience: range of practices.* Bank for International Settlements. https://www.bis.org/bcbs/publ/d454.pdf

Beckman, R. (2007). Profitability of Western European Banking Systems: Panel Evidence on Structural and Cyclical Determinants. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1090570

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of Cyber Risk – An Empirical Analysis. *The Geneva Papers on Risk and Insurance – Issues and Practice*, *40*(1), 1–25. https://doi.org/10.1057/gpp.2014.9

British Standards Institution. (2014). *Cybersecurity Standards – protecting networks, data and computers.* https://www.bsigroup.com/en-US/our-services/digital-trust/cybersecurity-information-resilience/cybersecurity-standards/

British Standards Institution. (2014). *Standards for IT and cyber security.* https://www.bsigroup.com/en-IN/Cyber-Security/standards-for-it-and-cyber-security/

Buith, J., & Spataru, D. (2016). The benefits and limits of cyber value-at-risk. *The Wall Street Journal*. https://deloitte.wsj.com/cio/the-benefits-limits-of-cyber-value-at-risk-1430712132

Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process.* CarnegieMellon.
https://insights.sei.cmu.edu/documents/786/2007_005_001_14885.pdf

Cavelty, M. D., & Smeets, M. (2023). Regulatory cybersecurity governance in the making: the formation of ENISA and its struggle for epistemic authority. *Journal of European Public Policy*, *30*(7), 1001–1020. https://doi.org/10.1080/13501763.2023.2173274

Cebula, J. J., & Young, L. R. (2010). *A Taxonomy of Operational Cyber Security Risks: Technical Note.* Software Engineering Institute. https://insights.sei.cmu.edu/library/a-taxonomy-of-operational-cyber-security-risks/Chakrabartty, S. N. (2017). Composite Index: Methods and Properties. *Journal of Applied Quantitative Methods*, 12(2), 12. https://www.researchgate.net/publication/321268796_Composite_Index_Methods_and_Properties

Chakraborty, S. (2007). TOPSIS and Modified TOPSIS: A comparative analysis. *Decision Analytics Journal*, *2*, 100021. https://doi.org/10.1016/j.dajour.2021.100021

Chang, A., Zhong, L., & Grabosky, P. (2018). Citizen co-production of cyber security: Self-help, vigilantes, and cybercrime. *Regulation & Governance*, *12*(1), 101–114. https://doi.org/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), 789–802. https://doi.org/10.1016/j.jbankfin.2007.09.017

Chavez-Demoulin, V., Embrechts, P., & Hofert, M. (2015). An Extreme Value Approach for Modeling Operational Risk Losses Depending on Covariates. *Journal of Risk and Insurance*, *83*(3), 735–776. https://doi.org/10.1111/jori.12059

Choi, S., & Kotrozo, J. (2006). Diversification, Bank Risk and Performance: A Cross-country Comparison. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1013430

Chubb Cyber Index. (n.d.). Providing Data-Driven Insight on Cyber Threat Trends. https://chubbcyberindex.com/#/incident-growth

Collier, B., Horgan, S., Jones, R., & Shepherd, L. (2020). The implications of the COVID-19 pandemic for cybercrime policing in Scotland: a rapid review of the evidence and future considerations. *Research Evidence in Policing: Pandemics*, 1, 1–18.
https://www.researchgate.net/publication/341742472_Issue_No_1_The_implications_of_the_COVID-19_pandemic_for_cybercrime_policing_in_Scotland_A_rapid_review_of_the_evidence_and_future_considerations

Cyber Intelligence and Information Security Center & Cyber Security National Lab. (2015). *2015 Italian Cyber Security Report: A National Cyber Security Framework*. CIS Sapienza & CINI. https://www.cybersecurityframework.it/sites/default/files/CSR2015_ENG.pdf

Cybersecurity Ventures Marcadet T. (2021). *Navigating through Cyber Risk. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/*

Dalal, R., Howard, D., Bennet, R., Posey, C., Zaccaro, S., & Brummel, B. (2021). Organizational science and cybersecurity: abundant opportunities for research at the interface. *Journal of Business and Psychology*, *37*, 1–29 https://doi.org/10.1007/s10869-021-09732-9

Deloitte Cyber Risk Services. (2016). European Conference on Cyber Warfare and Security, July, 145–154.

Deloitte. (2013). *Cyber risk and regulation in Europe. A new paradingm to banks.* https://www.deloitte.com/content/dam/Deloitte/lu/Documents/risk/lu_deloitte-cyber-risk-regulation-europe.pdf

Drayer, E. (2016). Resilient Distribution Grids – Cyber Threat Scenarios and Test Environment. In *2016 IEEE PES Innovative Smart Grid Technologies Conference Europe* (pp. 1–6). IEEE. https://doi.org/10.1109/ISGTEurope.2016.7856193

Eling, M., & Wirfs, J. H. (2016). *Cyber Risk: Too Big to Insure? Risk Transfer Options for a Mercurial Risk Class.* Institute of Insurance Economics, University of St. Gallen. https://www.econstor.eu/handle/10419/226644

Elkhannoubi, H., & Belaissaoui, M. (2015). A framework for an effective cybersecurity strategy implementation: Fundamental pillars identification. In *15th International Conference on Intelligent Systems Design and Applications* (pp. 1–6). IEEE. https://doi.org/10.1109/ISDA.2015.7489156

European Commission. (2005). *The Cybersecurity Strategy*. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

European Union. (2016, April 27). *Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR).* https://eur-lex.europa.eu/eli/reg/2016/679/oj

European Union. (2019, January 13). *Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02009L0138-20190113

Farid, G., Warraich, N. F., & Iftikhar, S. (2023). Digital information security management policy in academic libraries: A systematic review (2010–2022). *Journal of Information Science, 0*(0). https://doi.org/10.1177/01655515231160026

Ferreira, A. (2021). COVID-19 and Cybersecurity: Finally, an Opportunity to Disrupt. *JMIRx Med, 2*(2), e29517. doi:10.2196/21069

Fette, I., Sadeh, N., & Tomasic, A. (2007). Learning to detect phishing emails. In *Proceedings of the 16th International Conference on World Wide Web* (pp. 649–656). ACM. https://doi.org/10.1145/1242572.1242660

Galinec, D., & Možnik, D. (2017). Cybersecurity and cyber defence: national level strategic approach. *Automatika*, *58*(3), 273–286. https://doi.org/10.1080/00051144.2017.1407022

Gebre, S. L., Cattrysse, D., Alemayehu, E., & Van Orshoven, J. (2021). Multi-criteria decision-making methods to address rural land allocation problems: A systematic review. *International Soil and Water Conservation Research*, *9*(4), 490–501. https://doi.org/10.1016/j.iswcr.2021.04.005

Geneva Association. (2018). *Understanding and Addressing Global Insurance Protection Gaps. https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/understanding_and_addressing_global_insurance_protection_gaps.pdf*

Glorin, S. (2023). Do ChatGPT and Other AI Chatbots Pose a Cybersecurity Risk?: An Exploratory Study. *International Journal of Security and Privacy in Pervasive Computing (IJSPPC)*, *15*(1), 1–11. https://doi.org/10.4018/IJSPPC.320225

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security*, *5*(4), 438–457. https://doi.org/10.1145/581271.581274

Graziano, M., Cristalli, S., Pagnozzi, M., Lanzi, A., & Balzarotti, D. (2016). Micro-virtualization memory tracing to detect and prevent spraying attacks. In *Proceedings of the 25th USENIX Security Symposium* (pp. 431–446). USENIX Association. https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/cristalli

Graziano, M., Flore, L., & Lanzi, A. (2016). Subverting operating system properties through evolutionary DKOM attacks. In *Proceedings of the 13th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA'16), Vol. 9721* (pp. 3–24). Springer. https://doi.org/10.1007/978-3-319-40667-1_1

Greco, S., Ishizaka, A., Tasiou, M., & Torrisi, G. (2018). On the Methodological Framework of Composite Indices: A Review of the Issues of Weighting, Aggregation, and Robustness. *Social Indicators Research*, *141*, 61–94. https://doi.org/10.1007/s11205-017-1832-9

Grier, W. A. (2007). *Credit Analysis of Financial Institutions* (2nd ed.). Euromoney Institution Investor PLC.

Harjinder, S. L., Lynsay, A., Nurse, J., Erola, A., Epiphaniou, A., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*, 102248. https://doi.org/10.1016/j.cose.2021.102248

Hartmann, K., & Steup, C. (2013). The vulnerability of UAVs to cyber-attacks—an approach to the risk assessment. In *Proceedings of the 5th International Conference on Cyber Conflict* (pp. 1–23). NATO CCD COE. https://www.researchgate.net/publication/261449270_The_vulnerability_of_UAVs_to_cyber_attacks_-_An_approach_to_the_risk_assessment

Hasan, M. G., Ashraf, Z., & Khan, M. F. (2022). Multi-choice best-worst multi-criteria decision-making method and its applications. *International Journal of Intelligent Systems*, *37*(2), 1129–1156. https://doi.org/10.1002/int.22663

Heilman, S., & Kennedy-Phillips, L. (2011). Making Assessment Easier with the Organizational Effectiveness Model. *About Campus*, *15*(6), 29–32. https://doi.org/10.1002/abc.20046

Hiscox. (2017). *The Hiscox Cyber Readiness Report 2017.* Hiscox. https://www.hiscox.com/documents/brokers/cyber-readiness-report.pdf

Holler, M., Giffen, B., & Benzell, S. (2020, March). The General Data Protection Regulation in Financial Services Industries: How Do Companies Approach the Implementation of the GDPR and What Can We Learn from Their Approaches? [Conference Paper]. 82nd Annual Business Researchers Conference (VHB 2020), Frankfurt, Germany. https://www.researchgate.net/publication/340003405_The_General_Data_Protection_Regulation_in_Financial_Services_Industries_How_Do_Companies_Approach_the_Implementation_of_the_GDPR_and_What_Can_We_Learn_From_Their_Approaches

Home Office Science Advisory Council. (2018). *Understanding the costs of cybercrime: A report of key findings from the Costs of Cyber Crime Working Group, Research Report 96*. Home Office. https://assets.publishing.service.gov.uk/media/5a82d166e5274a2e8ab59814/understanding-costs-of-cyber-crime-horr96.pdf

Hubbard, D. W., & Seiersen, R. (2016). *How to Measure Anything in Cybersecurity Risk.* Wiley.

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

Hwang, C. L., & Yoon, K. (1981). Multiple Attribute Decision making – methods and applications: A State of the Art Survey. Springer Verlag.

IBM. (2012). *Reputational Risk and IT in the Banking Industry*. IBM. https://fst.net.au/wp-content/uploads/file/whitepaper/rlw03010usen_3.pdf

Ifinedo, P. (2022). Effects of Security Knowledge, Self-Control, and Countermeasures on Cybersecurity Behaviors. *Journal of Computer Information Systems*, *63*(2), 380–396. https://doi.org/10.1080/08874417.2022.2065553

International Monetary Fund. (2004, July 30). *Compilation Guide on Financial Soundness Indicators.* http://www.imf.org/external/np/sta/fsi/eng/2004/guide/index.htm/

ISACA. (2009). *The Risk IT framework.* Information Systems Audit and Control Association (ISACA).

ISACA. (2014). *The Cybersecurity Fundamentals Study Guide.* ISACA

Jaouadi, S., & Khemiri, S. (2012). Financial instability in Tunisia. *Global Advanced Research Journal of Management and Business Studies*, *2*(1), 044–049. http://garj.org/garjmbs/1/2013/2/1/financial-instability-in-tunisia-april-2012

Jaques, B., & Spataru, D. (2015). The benefits and limits of Cyber-Value-at-Risk. *The Wall Street Journal—Business.* https://deloitte.wsj.com/cio/the-benefits-limits-of-cyber-value-at-risk-1430712132

Jehovaness, A. (2008, March). Commercial Banks Efficiency in Tanzania [Conference Paper]. CSAE Conference on Economic Development in Africa, Oxford, UK.

Jitendra, J. (2017). A Recent Study over Cyber Security and its Elements. *International Journal of Advanced Research in Computer Science*, *8*(3), 791–793. https://doi.org/10.26483/ijarcs.v8i3.3099

Johnson, M. (2013). *Cyber Crime, Security and Digital Intelligence* (1st Ed.). Routledge.

Jouadi, S. (2014). Exploring effectiveness and efficiency of banks in Switzerland. *International Journal of Academic Research in Business and Social Sciences*, *4*(4), 313–325. https://doi.org/10.6007/IJARBSS/v4-i4/787

Jouini, M., Ben Arfa Rabai, L., & Ben Aissa, A. (2014). Classification of security threats in information systems. *Procedia Computer Science*, *32*, 489–496. https://doi.org/10.1016/j.procs.2014.05.452

Kaffenberger, L., Kopp, E., & Wilson, C. (2017). Cyber risk, market failures, and financial stability. *International Monetary Fund*, *2017*(185), 17–185. https://doi.org/10.5089/9781484313787.001

Karabacak, B., & Sogukpinar, I. (2005). ISRAM: information security risk analysis method. *Computers & Security*, *24*(2), 147–159. https://doi.org/10.1016/j.cose.2004.07.004

Kashyap, A. K., & Wetherilt, A. (2019). Some principles for regulating cyber risk. *AEA Papers and Proceedings*, *109*, 482–487. https://doi.org/10.1257/pandp.20191058

Kaspersky Lab. (2015). *Damage Control: The Cost of Security Breaches.* Kaspersky Lab. https://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf

Kleinknecht, A., Van Montfort, K., & Brouwer, E. (2002). The nontrivial choice between innovation indicators. *Economic Innovation and New Technologies*, *11*(2), 109–121. https://doi.org/10.1080/10438590210899

Kosmidou, K. (2008). The determinants of banks' profits in Greece during the period of EU Financial integration. *Journal of Managerial Finance*, *34*(3), 35–40. https://doi.org/10.1108/03074350810848036

Lahrmann, G., Marx, F., Mettler, T., Winter, R., & Wortmann, F. (2011). Inductive Design of Maturity Models: Applying the Rasch Algorithm for Design Science Research. In *Service-Oriented Perspectives in Design Science Research* (pp. 176–191). Springer. https://doi.org/10.1007/978-3-642-20633-7_13

Lent, N. T., & Hoang, D. B. (2016). Can maturity models support cyber security? In *2016 IEEE 35th International Performance Computing and Communications Conference* (pp. 1–7). IEEE. https://doi.org/10.1109/PCCC.2016.7820663

Li, T., Li, A., & Guo, X. (2020). The sustainable development-oriented development and utilization of renewable energy industry comprehensive analysis of MCDM methods. *Energy*, *212*, 118694. https://doi.org/10.1016/j.energy.2020.118694

McNeil, A. J., Frey, R., & Embrechts, P. (2015). *Quantitative Risk Management: Concepts, Techniques, Tools* (Revised Edition). Princeton University Press.

Mettler, T. (2011). Maturity assessment models: a design science research approach. *International Journal of Society Systems Science*, *3*(1/2), 81–98. https://doi.org/10.1504/IJSSS.2011.038934

Meyer, J. P., & Herscovitch, L. (2001). Commitment in the workplace: toward a general model. *Human Resource Management Review*, *11*(3), 299–326. http://dx.doi.org/10.1016/S1053-4822(00)00053-X

Mijwil, M. M., Ezzat Salem, I., & Ismaeel, M. M. (2023). The Significance of Machine Learning and Deep Learning Techniques in Cybersecurity: A Comprehensive Review. *Iraqi Journal for Computer Science and Mathematics*, *4*(1), 87–101. https://doi.org/10.52866/ijcsm.2023.01.01.008 Mouzas, S. (2006). Efficiency versus effectiveness in business networks. *Journal of Business Research*, *59*(10–11), 1124–1132. http://dx.doi.org/10.1016/j.jbusres.2006.09.018

Munda, G., & Nardo, M. (2005). *Constructing Consistent Composite Indicators: The Issue of Weights*. European Communities. https://core.ac.uk/download/pdf/38619689.pdf

Nardo, M., Saisana, M., Saltelli, A., Tarantola, S., Hoffman, A., & Giovannini, E. (2005). *Handbook on constructing composite indicators: methodology and user guide*. OECD. https://10.1787/533411815016 National Bank of Lithuania. (2023, December 22). *Survey: Cyberattacks pose the greatest risk to the financial system.* https://www.lb.lt/lt/naujienos/apklausa-finansu-sistemai-didziausia-rizika-kelia-kibernetines-atakos

National Bank of Lithuania. (2021). *Occasional Paper Series: Beyond the Traditional Unemployment Rate during Covid-19 in Lithuania.* https://www.lb.lt/uploads/publications/docs/33298_c9f4c21cf2731f213be75c49b1cd574a.pdf

National Cyber Security Center. (2019, October 23). *The NCSC Annual Review 2019*. https://www.ncsc.gov.uk/news/annual-review-2019

National Cyber Security Center. (2023, June 23). *Risk Management Guide*. https://www.ncsc.gov.uk/collection/risk-management

Klapkiv LNational Institute of Standards and Technology. (2004). *Standards for Security Categorization of Federal Information and Information Systems.* FIPS PUB 199. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

National Institute of Standards and Technology. (2004). *Standards for Security Categorization of Federal Information and Information Systems.* FIPS PUB 199. https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf

Naumov, S., & Kabanov, I. (2016). Dynamic framework for assessing cyber security risks in a changing environment. In *Proceedings of the 2016 International Conference on Information Science and Communications Technologies (ICISCT)* (pp. 1–4). IEEE. https://doi.org/10.1109/ICISCT.2016.7777406

Nelms, T., Perdisci, R., Antonakakis, M., & Ahamad, M. (2016). Towards Measuring and Mitigating Social Engineering Software Download Attacks. In *Proceedings of the 25th USENIX Security Symposium (USENIX Security'16)* (pp. 773–789). USENIX Association. https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_nelms.pdf

Nirmala, A. P., Asha, V., Ramesh, B. N., Chandana, K., Chandana, G. R., & Alam, A. (2023, January). A Systematic Review on classification of Cyber Attacks and its Prevention techniques to improve Cyber Security [Conference Paper]. 2023 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India. https://10.1109/ICCCI56745.2023.10128642

NIS Directive. (2023). Supporting the implementation of Union policy and law regarding cybersecurity. *Enisa*. https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new

NordLayer. (2023, September 29). *Evolution of cyber law: how the NIS2 Directive shapes Europe's security landscape. https://nordlayer.com/blog/how-nis2-directive-shapes-europes-security/*

OECD, European Union and European Commission, JRC. (2008). *Handbook on Constructing Composite Indicators: Methodology and User Guide*. OECD. https://doi.org/10.1787/9789264043466-en

OECD/Eurostat. (2018). *Oslo Manual 2018: Guidelines for Collecting, Reporting and Using Data on Innovation* (4th Edition). The Measurement of Scientific, Technological and Innovation Activities, OECD Publishing. https://doi.org/10.1787/9789264304604-en

Ongore, V., & Kusa, G. B. (2013). Determinants of Financial Performance of Commercial Banks in Kenya. *International Journal of Economics and Financial*

Issues, *3*(1), 237 252.https://www.econjournals.com/index.php/ijefi/article/view/334/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*(2), 445–455. https://doi.org/10.1016/S0377-2217(03)00020-1

Orlando, A. (2021). Cyber Risk Quantification: Investigating the Role of Cyber Value at Risk. *Risks*, *9*(10), 184. https://doi.org/10.3390/risks9100184

Ostroff, C., & Schmitt, N. (2017). Configurations of organizational effectiveness and efficiency. *Academy of Management Journal*, *36*(6), 1345–1361. DOI: 10.2307/256814

Patil, R., & Bharathi, S. V. (2022). A Study on the Business Transformation, Security Issues and Investors Trust in Fintech Innovation. *Cardiometry*, *24*, 918–932.

Pelissari, R., Khan, S. A., & Ben-Amor, S. (2022). Application of Multi-Criteria Decision-Making Methods in Sustainable Manufacturing Management: A Systematic Literature Review and Analysis of the Prospects. *International Journal of Information Technology & Decision Making*, *21*(02), 493–515. https://doi.org/10.1142/S0219622021300020

Pengelly, M. (2016, January 19). Cyber is the biggest operational risk fear, say practitioners. *Risk.net*. https://www.risk.net

Pinprayong, B., & Siengtai, S. (2012). Restructuring for organizational efficiency in the banking sector in Thailand: a case study of Siam Commercial Bank. *Far East Journal of Psychology and Business*, *8*(2), 29–42.

Ponemon Institute. (2012). *Cost of Cyber Crime Study: United States.* https://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf

Ponemon Institute. (2013). *Cost of Data Breach Study: Global Analysis*. https://www.ponemon.org/local/upload/file/2013%20Report%20GLOBAL%20CODB%20FINAL%205-2.pdf

Ponemon Institute. (2013). *Cost of Data Center Outages*. https://www.ponemon.org/local/upload/file/2013%20Cost%20of%20Data%20Center%20Outages%20FINAL%2012.pdf

Ponemon Institute. (2014). *Cost of Data Breach Study: Global Analysis*. https://centurybizsolutions.net/wp-content/uploads/2014/12/IBM.pdf

Ponemon Institute. (2015). *Cost of Data Breach Study: United States*. https://cdn2.hubspot.net/hubfs/360304/2015_Cost_Of_Data_Breach.pdf

Ponemon Institute. (2016). *Cost of Data Breach Study: Global Analysis*. https://www.cloudmask.com/hubfs/IBMstudy.pdf

Ponemon Institute. (2017). *Cost of Data Breach Study: Impact of Business Continuity Management.* IBM. https://www.logicalfront.com/wp-content/uploads/2018/01/BCM_Case_Study.pdf

Rabii, A., Assoul, S., Ouazzani Touhami, K., & Roudies, O. (2020). Information and cyber security maturity models: a systematic literature review. *Information and Computer Security*, *28*(4), 627–644. https://doi.org/10.1108/ICS-03-2019-0039

Radanlieva, P., De Roure, D. C., Nicolescu, R., Huth, M., Montalvo, R. M., Cannady, S., & Burnap, P. (2018). Future developments in cyber risk assessment for the Internet of Things. *Computers in Industry*, *102*, 14–22. https://doi.org/10.1016/j.compind.2018.08.002

RSI Security. (2023, May 16). *WHAT ARE CYBER CRIMES?* https://blog.rsisecurity.com/cyber-attacks/

Saeed, S., Altamimi, S., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. *Sensors*, *23*(15), 6666. https://doi.org/10.3390/s23156666

Sahoo, S. K., & Goswami, S. S. (2023). A Comprehensive Review of Multiple Criteria Decision-making (MCDM) Methods: Advancements, Applications, and Future Directions. *Decision Making Advances*, *1*(1), 25–48. https://doi.org/10.31181/dma1120237

Sahoo, S., & Goswami, S. (2024). Theoretical framework for assessing the economic and environmental impact of water pollution: A detailed study on sustainable development of India. *Journal of Future Sustainability*, *4*(1), 23–34. http://dx.doi.org/10.5267/j.jfs.2024.1.003

Sangmi, M., & Nazir, T. (2010). Analyzing Financial Performance of Commercial Banks in India: Application of CAMEL Model. *Pakistan Journal of Commerce and Social Science*, *4*(1), 46–48.

Santika, E., Fakhrughozy, M. H., Nur, W. M., & Lestar, H. S. (2022). Effect of Operational Risk on Financial Performance in Banking Industry IDX. *Jurnal Ekonomi*, *27*(1), 123–137. http://dx.doi.org/10.24912/je.v27i1.915

Santini, P., Gottardi, G., Baldi, M., & Chiaraluce, F. (2019). A Data-Driven Approach to Cyber Risk Assessment. *Data-Driven Cybersecurity*, *2019*, 6716918. https://doi.org/10.1155/2019/6716918

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a More Representative Definition of Cyber Security. Journal of Digital Forensics, Security and Law, 12(2), Article 8. https://doi.org/10.15394/jdfsl.2017.1476

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a More Representative Definition of Cyber Security. *Journal of Digital Forensics, Security and Law*, *12*(2017), 2–8. https://doi.org/10.15394/jdfsl.2017.1476

Schweitzer, N., Stulman, A., Shabtai, A., & Margalit, R. D. (2016). Mitigating denial of service attacks in OLSR protocol using fictitious nodes. *IEEE Transactions on Mobile Computing*, *15*(1), 163–172. https://doi.org/10.1109/TMC.2015.2409877

Scott, A. P., & Tierno, P. (2023). *Banking, Data Privacy, and Cybersecurity Regulation (R47434)*. Congressional Research Service. https://crsreports.congress.gov/product/details?prodcode=R47434

Shaikh, F. A., & Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Computers & Security*, *124*, 102974. https://doi.org/10.1016/j.cose.2022.102974

Sheth, A., Bhosale, S., & Kurupka, F. (2021). Research Paper on Cyber Security. *Contemporary Research in India (ISSN 2231-2137)*, 246–251.

Silber, J., Powers, E. V., & Fancher, J. (2021). *Beneath the surface of a cyberattack: A deeper look at business impacts.* Deloitte. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-beneath-the-surface-of-a-cyber-attack.pdf

Simanavičienė, R., & Petraitytė, V. (2016). Sensitivity analysis of the TOPSIS method in respect of initial data distributions. Lithuanian Journal of Statistics, 55(1), 45–51. Lietuvos statistikos darbai, 55(1), 45–51. https://www.statisticsjournal.lt. ISSN 2029-7262 online.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.

Singh, N., Krishnaswamy, V., & Zuopeng Zhang, J. (2023). Intellectual structure of cybersecurity research in enterprise information systems. *Enterprise Information Systems*, *17*(6), 2025545. https://doi.org/10.1080/17517575.2022.2025545

Srivastava, D., Singh, R., Chakraborty, C., Maakar, S., Maakar, A., & Sinwar, D. (2024). A framework for detection of cyber attacks by the classification of intrusion detection datasets. *Microprocessors and Microsystems*, *105*, 104964. https://doi.org/10.1016/j.micpro.2023.104964

Strohmier, H., Stoker, G., Vanajakumari, M., Clark, U., Cummings, J., & Modaresnezhad, M. (2022). Cybersecurity Maturity Model Certification Initial Impact on the Defense Industrial Base. *Journal of Information System Applied Research*, *15*(2), 17–29.

Strupczewski, G. (2021). Defining cyber risk. *Safety Science*, *135*, 105143. https://doi.org/10.1016/j.ssci.2020.105143

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

Sundarajan, V., & Errico, L. (2002). Islamic Financial Institutions and Products in the Global Financial System: Key Issues in Risk Management and Challenges Ahead.

Journal of Islamic Economics and Finance, *2002*(192), 18–23. https://doi.org/10.2139/ssrn.880303

Sunny, O. (2013). The Impact of Liquidity Management on the Profitability of Banks in Nigeria. *Journal of Finance and Bank Management*, *1*(1), 37–48.

Supriya, Y., & Gadekallu, T. R. (2023). A Survey on Soft Computing Techniques for Federated Learning: Applications, Challenges and Future Directions. *ACM Journal of Data and Information Quality*, *15*(2), 1–28. https://doi.org/10.1145/3575810

Tanaka, H., Matsuura, K., & Sudoh, O. (2005). Vulnerability and information security investment: An empirical analysis of e-local government in Japan. *Journal of Accounting and Public Policy*, *24*(1), 37–59. https://doi.org/10.1016/j.jaccpubpol.2004.12.003

Tehranipoor, M., & Koushanfar, F. (2010). A survey of hardware Trojan taxonomy and detection. *IEEE Design & Test of Computers*, *27*(1), 10–25. https://doi.org/10.1109/MDT.2010.7

The Crown Prosecution Service (CPS). (2019, September 26). *Cybercrime – Prosecution Guidance.* https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance Toch, E., Bettini, C., Shmueli, E., Radaelli, L., Lanzi, A., Riboni, D., & Lepri, B. (2018). The Privacy Implications of Cyber Security Systems: A Technological Survey. *ACM Computing Surveys*, *51*(2), 1–27. https://doi.org/10.1145/3172869

The White House. (2009). *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure.* National Security Archive. https://nsarchive.gwu.edu/document/21424-document-28

Ugur Aksu, M. Hadi Dilek, E. Islam Tatli. (2017). A quantitative CVSS-based cyber security risk assessment methodology for IT systems. In *International Carnahan Conference on Security Technology* (pp. 1–8). ICCST. https://doi.org/10.1109/CCST.2017.8167819

United Nations Office on Drugs and Crime. (2021). *COVID-19 vaccines and corruption risks: preventing corruption in the manufacture, allocation, and distribution of vaccines.* UNODC. https://www.unodc.org/documents/corruption/COVID-19/Policy_paper_on_COVID-19_vaccines_and_corruption_risks.pdf

Uyen, D. (2011). *The CAMEL rating system in banking supervision.* ARCADA. https://www.theseus.fi/bitstream/handle/10024/38344/Dang_Uyen.pdf

Vaughn, R., Henning, R., & Siraj, A. (2003). Information assurance measures and metrics: State of practice and proposed taxonomy. In *HICSS '03* (pp. 34–52). IEEE. https://doi.org/10.1109/HICSS.2003.1174904

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

Virglerova, Z., Panic, M. P., Voza, D., & Velickovic, M. (2021). Model of business risks and their impact on operational performance of SMEs. *Economic Research-Ekonomska Istraživanja*, *35*(1), 4047–4064. https://doi.org/10.1080/1331677X.2021.2010111

Walls, A., Perkins E., & Weiss J. (2013, June 7). Definition: "Cybersecurity". *Gartner. https://www.gartner.com/*

WEF. (2012). *Risk and Responsibility in a Hyperconnected World.* World Bank Group. (2020). *Financial Sector's Cybersecurity: A Regulatory Digest.* Financial Sector Advisory Center (FinSAC). https://thedocs.worldbank.org/en/doc/361881595872293851-0130022020/original/CybersecDigestv5Jul2020FINAL.pdf https://thedocs.worldbank.org/en/doc/361881595872293851-0130022020/original/CybersecDigestv5Jul2020FINAL.pdf

World Bank. (2016, July 1). *New Country Classifications by Income Level.* https://blogs.worldbank.org/opendata/new-country-classifications-2016

World Economic Forum. (2020). *The Global Risks Report 2020* (15th Ed.). WEF. http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf

World Economic Forum. (2023, January 18). *Global Cybersecurity OutlookGlobal Risks Report.* https://www.weforum.org/publications/global-cybersecurity-outlook-2023/

World Economic Forum. (2024, January 10). *Global Risks Report.* https://www.weforum.org/publications/global-risks-report-2024/digest/

Wu, W., Kang, R., & Li, Z. (2015). Risk assessment method for cyber security of cyber-physical systems. In *Proceedings of the 2015 First International Conference on Reliability Systems Engineering (ICRSE)* (pp. 1–5). IEEE. https://doi.org/10.1109/ICRSE.2015.7366430

Yenugula, M., Sahoo, S., & Goswami, S. (2024). Cloud computing for sustainable development: An analysis of environmental, economic, and social benefits. *Journal of Future Sustainability*, *4*(1), 59–66. http://dx.doi.org/10.5267/j.jfs.2024.1.005

Zavadskas, E. K., & Turskis, Z. (2011). Multiple Criteria Decision Making (MCDC) Methods in Economics: An overview. *Technological and Economic Development of Economy*, *17*(2), 397–427. https://doi.org/10.3846/20294913.2011.593291

Zhao, X., Xue, L., & Whinston, A. (2009). Managing Interdependent Information Security Risks: An Investigation of Commercial Cyber Insurance and Risk Pooling Arrangement. In *Thirtieth International Conference on Information Systems* (pp. 189–239). DBLP.

Zhou, C. V., Leckie, C., & Karunasekera, S. (2010). A survey of coordinated attacks and collaborative intrusion detection. *Computers & Security*, *29*(1), 124–140. https://doi.org/10.1016/j.cose.2009.06.008

List of Scientific Publications by the Author on the Topic of the Dissertation

Papers in the Reviewed Scientific Journals

Gavėnaitė-Sirvydienė, J., & Miečinskienė, A. (2023a) A framework for cyber security areas evaluation in financial sector. *Transformations in Business and Economics, 22*, 3(60), 192–205. http://www.transformations.knf.vu.lt/60/article/afra

Gavėnaitė-Sirvydienė, J., & Miečinskienė, A. (2023b) The assessment of cyber security's significance in the financial sector of Lithuania. *Journal of cyber security and mobility: River Publishers,* 12(4), 497–518. https://doi.org/10.13052/jcsm2245-1439.1243

Papers in Other Editions

Gavėnaitė-Sirvydienė, J., & Miečinskienė, A. (2021). Forecasting costs of cyber-attacks using estimation of the global cost of cyber risk calculator V 1.2. In *International scientific conference "Contemporary issues in business, management and economics engineering 2021"* (pp. 1-9). VGTU. https://doi.org/10.3846/cibmee.2021.618

Gavėnaitė-Sirvydienė, J. (2022). COVID-19 global pandemic impact on cyber security in the financial institutions. In *Building strategic resilience in times of uncertainty: Proceedings of 15th annual scientific Baltic business management conference* (pp. 22–26). ASBBMC. https://www.ba.lv/wp-content/uploads/2015/08/proceedings-asbbmc_22.pdf

Summary in Lithuanian

Įvadas

Problemos formulavimas

Verslo aplinka ir ekonomika tampa vis labiau priklausomos nuo informacinių technologijų (IT), kurios yra plačiai integruojamos į įvairias verslo sritis ir procesus (Eling et al., 2023). Europos centrinio banko duomenimis, kasmet kibernetinių atakų sukelti nuostoliai visame pasaulyje viršija 200 mlrd. JAV dolerių, o kibernetinė rizika pripažįstama viena iš svarbiausių rizikų finansų sistemos stabilumui (Europos Centrinis Bankas, 2024). Pagrindiniai kibernetinių atakų sukeliami padariniai yra finansiniai nuostoliai, žala reputacijai, prarasti klientai ir jų pasitikėjimas bei lojalumas, sugadintos įmonės naudojamos operacinės sistemos arba netgi įmonės veiklos nutrūkimas.

Naujų technologijų, tokių kaip dirbtinis intelektas, didžiųjų duomenų integravimas į finansinių institucijų veiklos procesus padidino institucijų kibernetinį pažeidžiamumą (Saeed et al., 2023). Kasdien finansų sektoriuje sukuriamas didžiulis kiekis duomenų, apimančių viską – nuo duomenų apie klientus iki sandorių istorijos (Ahmadi, 2024). Kibernetinių rizikų identifikavimas ir kibernetinio saugumo situacijos analizė padeda įvertinti kibernetinio saugumo lygį finansų institucijoje (Fairford & Jembei, 2023). Siekdamos apsaugoti sistemas, jautrią informaciją, vidines duomenų bazes nuo galimų kibernetinių rizikų, finansų institucijos turi diegti vidinę kibernetinių rizikų vertinimo ir valdymo tvarką. Šios tvarkos kūrimas bei papildomos priemonės kibernetinės rizikos

vertinimui ir mažinimui reikalauja papildomų žmogiškųjų išteklių bei laiko ir finansinių investicijų (Kamiya et al., 2021).

Pasak Pasaulio Ekonomikos Forumo ataskaitos, kibernetinės atakos yra viena iš penkių didžiausių rizikų, su kuriomis per pastaruosius kelerius metus susidūrė vyriausybės ir įmonės visame pasaulyje (World Economic Forum, 2024). Finansų institucijos tampa vis patrauklesnės kibernetiniams nusikaltėliams dėl savo veiklos specifikos, duomenų jautrumo ir nuolatinės elektroninių paslaugų plėtros. Dėl šių priežasčių itin svarbu imtis tinkamų priemonių, kurios leistų vertinti kibernetines rizikas ir kibernetinio saugumo lygį finansų institucijose.

Siekdamos užtikrinti veiklos tęstinumą ir saugumą, finansų institucijos turi diegti naujus procesus, kurie leistų įvertinti kibernetinio saugumo lygį organizacijoje (Patil et al., 2022). Kibernetinio saugumo vertinimo problema yra reikšminga ir turi būti sprendžiama. Šiuo metu nėra pasiūlyta tinkama priemonė, kuri leistų įvertinti kibernetinio saugumo lygį išskirtinai finansų institucijoje, analizuojant specifines sritis, rizikas ar konkrečius kibernetinio saugumo iššūkius, su kuriais susiduria būtent finansinės institucijos.

Darbo aktualumas

Elektroninės finansinės paslaugos yra neatsiejama kasdienio gyvenimo dalis, todėl kibernetinė rizika finansų institucijoms yra viena naujausių ir pavojingiausių. Lietuvos Banko atlikto tyrimo duomenimis, kibernetinių grėsmių galimybė ir poveikis Lietuvos finansų sistemai yra viena aktualiausių problemų, kurią artimiausiais metais reikėtų įvardyti kaip prioritetinę (Lietuvos Bankas, 2023). Europos Sąjungos direktyvoje dėl priemonių, užtikrinančių aukštą kibernetinio saugumo lygį visoje Europoje (NIS2 direktyva, 2023), daug dėmesio skiriama duomenų apsaugai ir kibernetiniam saugumui, kibernetinės rizikos tyrimus ir vertinimą laikant vienomis svarbiausių priemonių kibernetiniam saugumui užtikrinti. Dėl veiklos specifikos, ypatingo jautrių duomenų pažeidžiamumo, griežto teisinio reguliavimo ir finansinių nuostolių grėsmės finansų institucijoje kibernetinių rizikų ir kibernetinio saugumo vertinimas yra ypatingai aktualus.

Tyrimo objektas

Disertacijos tyrimo objektas - kibernetinio saugumo vertinimas finansų institucijose.

Darbo tikslas

Disertacijos darbo tikslas - sukurti kibernetinio saugumo vertinimo priemonę, kuri leistų įvertinti kibernetinio saugumo lygį finansų institucijose.

Darbo uždaviniai

Nustatytam tikslui pasiekti keliami šie uždaviniai:

1. Išanalizuoti kibernetinės rizikos ir kibernetinio saugumo ypatumus bei svarbą ir nustatyti pagrindines kibernetinio saugumo sritis ir rodiklius, atspindinčius svarbiausius kiekvienos srities bruožus teoriniu aspektu.

2. Sukurti metodiką priemonei, leidžiančiai įvertinti finansų institucijos kibernetinį saugumą.
3. Sudaryti unikalų klausimyną, skirtą vidiniam kibernetinio saugumo lygio finansų institucijoje įvertinimui atlikti, remiantis pateiktais kibernetinio saugumo rodikliais.
4. Sukurti finansų institucijų kibernetinio saugumo vertinimo priemonę, kaip galutinį rezultatą pasiūlant sudėtinį kibernetinio saugumo indeksą.
5. Įvertinti kibernetinio saugumo lygį pasirinktose finansų institucijose ir taip praktiškai patikrinti siūlomą sudėtinį kibernetinio saugumo indeksą.

Tyrimų metodika

Rengiant disertaciją buvo naudojami įvairūs metodai:

- kritinė mokslinės literatūros analizė ir sisteminimas, siekiant pateikti kibernetinio saugumo sampratą, aptarti jo ypatumus ir svarbą finansų įstaigoms;
- pasaulinių kibernetinių rizikų kaštų skaičiuoklė (angl. *global cyber risks costs calculator*) kaip įrankis galimai finansinei kibernetinės rizikos reikšmei finansų institucijoms įvertinti;
- daugiakriteriniai sprendimų priėmimo metodai, tokie kaip paprastasis pridėtinių svorių metodas (SAW) ir pirmenybės tvarkos pagal panašumą į idealų sprendimą metodas (TOPSIS), skirti kibernetinių rizikų reikšmingumui ir kibernetinio saugumo rodiklių svoriams nustatyti;
- ekspertų interviu, siekiant surinkti kokybinius duomenis kibernetinio saugumo reikšmingumui įvertinti ir pagrindiniams kibernetinio saugumo rodikliams nustatyti;
- OECD sudėtinio indekso sudarymo metodika, kuri apima dešimt etapų, įskaitant duomenų atranką, priskyrimą, daugiamatę analizę, normalizavimą, svorių nustatymą ir neapibrėžtumo analizę.

Darbo mokslinis naujumas

Disertacijoje pateikiami šie nauji ekonomikos mokslų rezultatai:

1. Atlikus išsamią mokslinės literatūros analizę, nustatytos keturios pagrindinės kibernetinio saugumo sritys – teisinė, organizacinė, techninė ir incidentų valdymo, taip pat nustatyti konkretūs rodikliai, apibūdinantys kiekvieną iš šių sričių išskirtinai finansų institucijose.
2. Atlikus ekspertų interviu ir taikant MCDM metodus buvo nustatyti kiekvieno iš 22 rodiklių svoriai, apibūdinantys jų svarbą bendrame finansų institucijų kibernetinio saugumo sričių kontekste.
3. Siejant mokslinės literatūros analizės ir ekspertų vertinimų rezultatus, buvo sukurtas originalus klausimynas, leidžiantis finansų institucijoms atlikti vidinį kiekvieno kibernetinio saugumo rodiklio įvertinimą.

4. Sukurtas sudėtinis finansų institucijų kibernetinio saugumo indeksas. Ši nauja priemonė gali būti naudojama kaip veiksmingas įrankis finansų institucijų kibernetiniam saugumui vertinti. Ekonominiu požiūriu indeksas gali būti naudojamas kaip priemonė reikalingoms investicijoms į kibernetinį saugumą planuoti.
5. Ekonomikos mokslo požiūriu sudėtinis kibernetinio saugumo indeksas yra nauja išsami priemonė, skirta kibernetinei rizikai finansų institucijose įvertinti ir sumažinti.

Praktinė tyrimo rezultatų vertė

Sukurta ir empiriškai patikrinta originali finansų institucijų kibernetinio saugumo vertinimo priemonė (sudėtinis kibernetinio saugumo indeksas) gali būti naudojama finansų institucijose jų kibernetinio saugumo lygiui įvertinti. Be to, šis pasiūlytas įrankis galėtų būti labai naudingas nustatant institucijų pažeidžiamumą ir silpnąsias vietas konkrečiose srityse. Jis galėtų būti vertinimo matas, pagal kurį būtų galima nustatyti tobulinimo ir investicijų paskirstymo kryptis, siekiant didinti saugumo lygį. Sudėtinis kibernetinio saugumo indeksas galėtų būti naudojamas bet kurioje finansų institucijoje, taip pat jis galėtų būti naudojamas kaip vieninga bendra matavimo priemonė, leidžianti palyginti skirtingų institucijų rezultatus bei įvertinti bendrą visos finansų sistemos kibernetinio saugumo lygį.

Ginamieji teiginiai

1. Teorinį pagrindą sudėtiniam kibernetinio saugumo indeksui sudaryti sukuria sisteminis požiūris į kibernetines rizikas, kibernetinio saugumo ypatumus ir tai leidžia nustatyti pagrindines kibernetinio saugumo sritis ir rodiklius būtent finansų institucijoms.
2. Originalus klausimynas, skirtas vidiniam kibernetinio saugumo sričių ir rodiklių vertinimui atlikti, leidžia įvertinti kibernetinio saugumo situaciją finansų institucijoje ir yra reikalinga sudėtinio kibernetinio saugumo indekso dalis.
3. Pagrindinių kibernetinio saugumo sričių, rodiklių, jų konkrečių svorių ir finansų institucijos vidinio vertinimo rezultatai leidžia sudaryti sudėtinį indeksą finansų institucijos kibernetinio saugumo lygiui įvertinti.
4. Sudėtinis kibernetinio saugumo indeksas yra tinkama priemonė finansų institucijos kibernetinio saugumo lygiui vertinti, taip pat jis gali būti naudojamas skirtingų institucijų rezultatams tarpusavyje palyginti.

Darbo rezultatų aprobavimas

Disertacijos tema publikuoti keturi moksliniai straipsniai: 2 – tarptautiniuose recenzuojamuose mokslo žurnaluose, iš kurių vienas įtrauktas į *Scopus* duomenų bazę (Gavėnaitė-Sirvydienė & Miečinskienė, 2023a; Gavėnaitė-Sirvydienė & Miečinskienė,

2023b) pateikiančią cituojamumo rodiklį, 2 – tarptautinių konferencijų medžiagose (Gavėnaitė-Sirvydienė & Miečinskienė, 2021; Gavėnaitė-Sirvydienė, 2022)

Disertacijoje atliktų tyrimų rezultatai buvo paskelbti dviejose tarptautinėse mokslinėse konferencijose:

- 15-oji kasmetinė mokslinė Baltijos šalių verslo vadybos konferencija „Building Strategic Resilience in Times of Uncertaint“. 2022, birželio 1d., Ryga, Latvija;
- „Contemporary Issues on Business, Management and Economics Engineering“. 2021, gegužės 13 d., Vilnius, Lietuva.

Autorius taip pat skaitė keturis pranešimus Vilniaus Gedimino technikos universiteto doktorantūros seminaruose ir vieną pranešimą tarptautiniame seminare Latvijoje (*BA School of Business and Finance*).

Disertacijos struktūra

Disertaciją sudaro trys skyriai: pirmajame disertacijos skyriuje analizuojama kibernetinio saugumo samprata, pateikiamas sisteminis požiūris į kibernetinio saugumo komponentus. Antrasis disertacijos skyrius skirtas metodikai, pagal kurią bus sudarytas kibernetinio saugumo indeksas, sukurti. Trečiajame skyriuje pateikiamas tyrimo rezultatas – sudėtinis finansų institucijos kibernetinio saugumo indeksas. Taip pat pateikiami ir indekso praktinio aprobavimo rezultatai bei palyginami trijų realių finansų institucijų kibernetinio saugumo indeksų rezultatai.

1. Kibernetinių rizikų ir kibernetinio saugumo teoriniai aspektai

Šiame skyriuje nagrinėjamos teorinės kibernetinio saugumo ir kibernetinių rizikų prielaidos. Išanalizavus atrinktą mokslinę literatūrą, pirmajame skyriuje pateikiama išsami kibernetinio saugumo sampratos, esminių kibernetinio saugumo požymių, jų svarbos ir galimo poveikio finansų institucijai apžvalga. Detaliai nagrinėjama kibernetinio saugumo struktūra, analizuojami skirtingi požiūriai į kibernetinio saugumo sudedamąsias dalis, kibernetinio saugumo lygio įvertinimo procesus ir svarbą, finansų institucijoms būdingas teisinio reguliavimo ir duomenų apsaugos prielaidas. Atlikta mokslinės literatūros analize siekiama svariai pagrįsti tolesniuose skyriuose atliekamus tyrimus, kuriuose pagrindinis dėmesys skiriamas finansų institucijų kibernetinio saugumo lygiui įvertinti.

Apibendrinta kibernetinio saugumo samprata apima keletą esminių sričių, tokių kaip (Dalal et al., 2021; Georgiadou et al., 2022; Kianpour et al., 2022):

1. galimybę apsaugoti verslo aplinką nuo kibernetinių atakų;
2. informacijos prieinamumo ir konfidencialumo verslo aplinkoje pažeidimų prevenciją;
3. pastangas visas priemonės ir veiksmus skirti jautrios informacijos, duomenų ir kibernetinės erdvės apsaugai;

4. rizikos ir galimos žalos prevenciją, siekiant apsaugoti ir prireikus atkurti informaciją, duomenis, duomenų saugyklas, elektroninių ryšių sistemas ir paslaugas.

Kibernetinės atakos vis dar išlieka viena aktualiausių verslo rizikų (Pasaulio ekonomikos forumas, 2024). Nors kibernetinės rizikos ar kibernetinio saugumo lygio įvertinimas gali būti gana sudėtingas, jis labai svarbus verslo tęstinumui, finansų institucijos reputacijai ir pelningumui.

Kibernetinės rizikos vertinimas yra viena iš svarbiausių kibernetinio saugumo aplinkos sudedamųjų dalių. Siekdami apsaugoti svarbiausius ir pažeidžiamiausius verslo procesų elementus, kibernetinės rizikos tyrimai ir vertinimas skatina inovacijas bei kibernetinio saugumo plėtrą (Luburic, 2019).

Kibernetinės rizikos vertinimo procesas yra vienas iš esminių veiksnių kuriant ir įgyvendinant veiksmingą finansų institucijos kibernetinio saugumo strategiją. Siekiant užtikrinti, kad finansų institucijos įgyvendinamos saugumo priemonės yra tinkamos apsisaugoti nuo kibernetinių grėsmių, būtina visapusiškai suvokti kibernetinio saugumo vertinimo esmę (Santini et al., 2019). Vertinant rizikos lygį reikėtų atsižvelgti į įvairius veiksnius, įskaitant (CISA, 2022):

1. prielaidų, kuriomis grindžiamas skirstymas į „didelės“, „vidutinės“ ir „mažos“ rizikos kategorijas, paaiškinimą;
2. nuoseklias ir tikslias tokių terminų kaip „rizika“ ir „grėsmė“ apibrėžtis;
3. turto, prietaisų, sistemų, kurioms kibernetinės atakos atveju būtų padaryta žala, ir duomenų, kurie tokiu atveju būtų pažeisti, nustatymą;
4. konkrečių kibernetinių rizikų, nukreiptų į įvardytą turtą, duomenis ir kt., nustatymą;
5. esamų kontrolės priemonių veiksmingumo kibernetiniams pažeidimams mažinti įvertinimą;
6. institucijos personalo pasirengimo reaguoti į kibernetinius incidentus lygio įvertinimą.

Nacionalinio standartų ir technologijų instituto (NIST) kibernetinio saugumo sistema yra viena iš žinomiausių rizikos vertinimo sistemų. Ši sistema siūlo organizacijoms lanksčias ir struktūruotas gaires, kad jos galėtų įvertinti savo kibernetinio saugumo riziką ir nustatyti prioritetinius veiksmus šiai rizikai sumažinti. NIST kibernetinio saugumo sistemą sudaro penki pagrindiniai elementai (S1.1 lentelė):

S1.1 lentelė. NIST kibernetinio saugumo sistemos elementai. Sudaryta autorės, remiantis NIST kibernetinio saugumo sistema 2.0 (2023 m.).

Kibernetinio saugumo elementas	Aprašymas
Identifikuoti	Nustatyti bazinę organizacijos saugumo būklę ir identifikuoti riziką.
Saugoti	Įgyvendinti saugumo kontrolės priemones.
Atrasti	Sukurti ir įgyvendinti procesus kibernetinio saugumo incidentams nustatyti.

S1.1 lentelės pabaiga

Kibernetinio saugumo elementas	Aprašymas
Reaguoti	Sukurti ir įgyvendinti reagavimo į nustatytus kibernetinio saugumo incidentus planus.
Atstatyti	Parengti ir įgyvendinti sistemų ir duomenų atkūrimo po kibernetinio saugumo incidento planus.

Literatūros analizė įrodė, kad kibernetinių pažeidimų pasekmės tiesiogiai susijusios su kibernetinės rizikos rūšimi. Kadangi yra įvairių metodų ir būdų, kaip klasifikuoti kibernetinę riziką, galimos pasekmės ir žala gali būti skirtingos. Finansų sektoriaus institucijos (bankai, draudimo bendrovės, kredito unijos, investicinės bendrovės, finansų maklerio įmonės ir kitos) kibernetinio saugumo kontekste yra vienos svarbiausių ir pažeidžiamiausių. Dėl plataus spektro itin jautrios informacijos ir duomenų, kuriais disponuoja finansų institucijos, jų pažeidžiamumas kibernetinės rizikos kontekste yra vienas didžiausių.

Taigi, remiantis atlikta mokslinės literatūros analize, susijusia su finansų institucijų kibernetiniu saugumu, daroma išvada, kad siekdamos užtikrinti saugias finansines paslaugas, atitinkančias įvairius teisinius reikalavimus, finansų įstaigos turi imtis veiksmų, susijusių su kibernetinės rizikos identifikavimo, valdymo ir vertinimo procesais.

2. Metodika, skirta sukurti priemonę finansų institucijų kibernetiniam saugumui įvertinti

Šiame disertacijos skyriuje aptariama empirinių ir statistinių tyrimų, kuriais remiantis kuriamas sudėtinis finansų institucijos kibernetinio saugumo indeksas, metodologija. Taip pat šiame skyriuje tiriami galimi kibernetinės rizikos, kibernetinės rizikos reikšmingumo ir finansinės kibernetinių rizikų žalos vertinimo metodai, modelis, skirtas esminėms kibernetinio saugumo sritims ir finansų institucijos kibernetinio saugumo rodikliams nustatyti, bei metodai sudėtiniam indeksui sudaryti.

Taikant daugiakriterinį ekspertinių sprendimų analizės metodą (TOPSIS), buvo įvertinta finansų sektoriaus įmonių kibernetinio saugumo svarba (S2.1 lentelė). Siekiant tirti vertingus ir patikimus duomenis, ekspertams buvo iškelti šie reikalavimai:

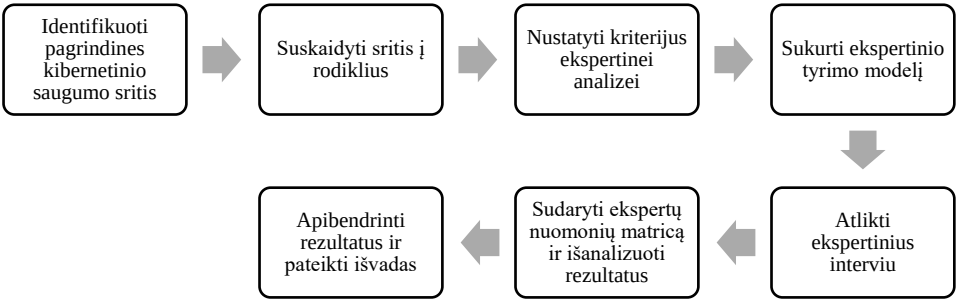
1. finansų institucijos (banko arba draudimo bendrovės) atstovavimas;
2. ne mažesnė kaip dešimties metų patirtis finansų srityje;
3. vadovo pareigos vienoje iš šių sričių: IT saugumo, duomenų apsaugos, rizikos valdymo.

Respondentai buvo atrinkti iš šešių Lietuvoje veikiančių organizacijų (bankų ir draudimo bendrovių).

S2.1 lentelė. Ekspertinio vertinimo kibernetinio saugumo svarbai nustatyti struktūra (sudaryta autorės)

Kriterijus	Alternatyvos
Svarbiausia kibernetinio saugumo sritis organizacijoje	Duomenų saugumas Tinklo saugumas Mobiliojo ryšio saugumas Duomenų bazių ir infrastruktūros saugumas Galutinių naudotojų mokymas Debesų saugumas Duomenų ir sistemų atkūrimas po incidentų ir veiklos tęstinumas
Kenksmingiausia kibernetinių rizikų rūšis organizacijoje	Duomenų pasisavinimas apgaulės būdu (angl. *phishing*) Paskyros perėmimo ir piktnaudžiavimo įgaliojimais atakos Kenkėjiška programinė įranga (virusai, kirminai, Trojos arkliai) Interneto programų atakos Vidinės grėsmės Išpirkos reikalaujančios programos Paslaugų trikdymo (DoS/DDoS) atakos
Organizacijoje labiausiai tikėtinas kibernetinės atakos tipas	Duomenų išviliojimas (angl. *phishing*) Kenkėjiška programinė įranga Išpirkos reikalaujančios programos Interneto programų atakos Paskyros perėmimo ir piktnaudžiavimo įgaliojimais atakos Vidinės grėsmės Atsisakymas teikti paslaugas
Kibernetinės rizikos, kurioms organizacija yra geriausiai pasiruošusi	Kenkėjiška programinė įranga Vidinės grėsmės Paskyros perėmimo ir piktnaudžiavimo įgaliojimais atakos Duomenų išviliojimas (angl. *phishing*) Interneto programų atakos Išpirkos reikalaujančios programos Atsisakymas teikti paslaugas
Kibernetinių atakų svarba ir reikšmė kitų esamų finansinių ir veiklos rizikų, susijusių su jų verslu, kontekste	Finansinė rizika (likvidumo, kredito, mokesčių) Kibernetinė rizika Rinkos rizika (nuosavybės vertybinių popierių, palūkanų normos, valiutos) Operacinė rizika (pardavimai, rinkodara, žmonės) Atitikties rizika (reguliavimo, teisinė) Strateginė rizika (komunikacijos, investavimo, išteklių)

Siekiant sukurti įrankį, skirtą finansų institucijos kibernetiniam saugumui įvertinti, būtina įvertinti pagrindines kibernetinio saugumo sritis. Efektyvią rizikos valdymo strategiją galima sukurti ir įgyvendinti konkrečiai nustačius finansų institucijoje svarbiausias kibernetinio saugumo sritis ir kriterijus.



S2.1 pav. Pagrindinių kibernetinio saugumo sričių nustatymo schema (sudaryta autorės)

Taikant daugiakriterinės ekspertinės sprendimų analizės metodą (SAW), buvo įvertinta kibernetinio saugumo sričių ir jų rodiklių svarba finansų sektoriaus įmonėse. Siekiant surinkti patikimus duomenis, ekspertams buvo nustatyti šie reikalavimai:

1. ekspertas turi atstovauti finansų įstaigai (bankui arba draudimo bendrovei);
2. ekspertas turi turėti ne mažesnę kaip penkerių metų patirtį finansų srityje;
3. ekspertas turi užimti vadovo pareigas vienoje iš šių sričių: IT saugumo, duomenų apsaugos, rizikos valdymo.

Ekspertų klausimynas apėmė keturias skirtingas finansų įstaigos kibernetinio saugumo sritis. Šios sritys buvo pasirinktos remiantis mokslinės literatūros analizės ir duomenų apibendrinimo rezultatais, nustatant esminius aspektus, susijusius su finansų įstaigos kibernetiniu saugumu (S2.2 lentelė):

1. teisinės priemonės;
2. organizacinės priemonės;
3. techninės priemonės;
4. incidentų valdymas.

S2.2 lentelė. Ekspertinio vertinimo struktūra pagrindinėms kibernetinio saugumo sritims ir rodikliams nustatyti (sudaryta autorės)

Sritis	Rodiklis
Teisinės priemonės	Įmonės vidaus politika ir (arba) gairės
Teisinės priemonės	Tarptautiniai teisiniai reikalavimai (ES lygmeniu)
Teisinės priemonės	Atitikties ir kibernetinio saugumo standartų užtikrinimas
Teisinės priemonės	Pagrindinių atitikties rodiklių ataskaitos
Organizacinės priemonės	Kibernetinės rizikos vertinimas ir prioritetų nustatymas
Organizacinės priemonės	Vidaus kibernetinės rizikos kontrolė
Organizacinės priemonės	Mokymai ir naudotojų švietimas
Organizacinės priemonės	Investicijos į kibernetinio saugumo plėtrą
Organizacinės priemonės	Atskaitingo pareigūno skyrimas (komanda)
Organizacinės priemonės	Strateginis požiūris į kibernetinę riziką

S2.2 lentelės pabaiga

Sritis	Rodiklis
Techninės priemonės	Kibernetinių grėsmių, susijusių su galimais nuostoliais, vertinimas
Techninės priemonės	Konkrečios saugumo sistemos
Techninės priemonės	Trečiųjų šalių atsakomybė už kibernetinį saugumą
Techninės priemonės	Galimų kibernetinių atakų motyvų nustatymas
Techninės priemonės	Prieiga prie neskelbtinų duomenų ir vidaus sistemų
Incidentų valdymas	Draudimas nuo kibernetinių rizikų
Incidentų valdymas	Pranešimo mechanizmas pažeidimo ir kibernetinės atakos atveju
Incidentų valdymas	Veiksmų peržiūros ir testavimas
Incidentų valdymas	Reagavimo į kibernetinius incidentus padalinys
Incidentų valdymas	Kibernetinių krizių valdymo planas
Incidentų valdymas	Priemonės ir įrankiai, skirti pasekmėms mažinti
Incidentų valdymas	Atsigavimas po kibernetinio incidento

Kibernetinio saugumo indeksas galėtų būti veiksminga finansų institucijų priemonė savo lygiui šioje srityje įvertinti bei pažeidžiamoms vietoms ir trūkstamoms galimybėms atrasti, o tai padėtų teikti verslui nuolatinę paramą saugumo srityje. Todėl bendroji šios priemonės sistema ir tikslai apima kelias skirtingas kibernetinio saugumo sritis, jų rodiklius, rodiklių svorius ir individualius kiekvienos finansų institucijos rezultatus, įvertinant kiekvieno iš rodiklių vertę (S2.4 lentelė).

S2.3 lentelė. Nustatyta sudėtinio kibernetinio saugumo indekso sandara (sudaryta autorės)

SRITIS	RODIKLIS	RODIKLIO SVORIS	INDIVIDUALUS INSITITUCIJOS REZULTATAS
TEISINĖS PRIEMONĖS	4 specifiniai srities rodikliai	Individualus kiekvieno rodiklio svoris	Individualus institucijos kiekvieno rodiklio įsivertinimo rezultatas
ORGANIZACINĖS PRIEMONĖS	6 specifiniai srities rodikliai		
TECHNINĖS PRIEMONĖS	5 specifiniai srities rodikliai		
INCIDENTŲ VALDYMAS	7 specifiniai srities rodikliai		

Finansų institucijoms skirtas kibernetinio saugumo indeksass suskirstytas į keturias pagrindines sritis, kurios vėliau suskirstomos į 22 rodiklius. Siekiant veiksmingai įvertinti kibernetinio saugumo būklę, kiekvienam rodikliui priskiriamas individualus svoris, kuris nustatomas atskiro tyrimo metu.

Atlikus įvairių metodų, susijusių su kibernetinėmis rizikomis ar kibernetinio saugumo vertinimu analizę, paaiškėjo, kad apskritai kibernetinio saugumo koncepcija yra

daugialypė problema, apimanti daugybę sričių ir klausimų, todėl konkretiems tyrimo tikslams pasiekti reikėtų pasirinkti konkretų metodą.

Finansų institucijos kibernetinio saugumo lygio vertinimas gali būti grindžiamas įvairiais požiūriais ir aplinkybėmis. Remiantis atliktais moksliniais tyrimais buvo atrinkti tolesniems tyrimams ir sudėtiniam indeksui konstruoti tinkamiausi metodai:

- daugiakriteriniai sprendimų priėmimo metodai (angl. multi-criteria decision-making method) TOPSIS ir SAW, skirti ekspertų vertinimų duomenims apdoroti;
- min / max reikšmių metodas duomenų normalizavimo etapui užbaigti;
- EBPO metodika, skirta sudėtiniam indeksui konstruoti.

Tokie indeksai kaip Nacionalinis kibernetinio saugumo indeksas (pagal kurį nustatomas šalies kibernetinio saugumo lygis), Kibernetinio atsparumo indeksas (pagal kurį lyginamas šalių pasirengimas ir atsparumas) ir Pasaulinis kibernetinio saugumo indeksas (pagal kurį lyginamas šalių kibernetinio saugumo lygis) orientuoti į nacionalinį arba pasaulinį lygį. Jie padeda šalims identifikuoti pažeidžiamas sritis ir didinti kibernetinį saugumą nacionaliniu lygmeniu, taip pat leidžia jį palyginti tarptautiniame kontekste. Todėl šis naujas siūlomas indeksas bus skirtas išskirtinai tik finansų institucijoms ir atspindės sritis ir rodiklius, kurie susiję su šia finansų sritimi.

3. Sudėtinio finansų institucijų kibernetinio saugumo indekso sudarymas

Šiame skyriuje pateikiami finansų sektoriaus kibernetinio saugumo svarbos vertinimo rezultatai. Šie rezultatai kartu su galimų kibernetinės rizikos sukeltų kaštų prognoze bei esminių kibernetinio saugumo sričių, rodiklių ir jų svorių rezultatais sudaro tvirtą ir reikšmingą sudėtinio kibernetinio saugumo indekso pagrindą. Sudarius kibernetinio saugumo indeksą, jis naudojamas faktiniams indekso balams trijose skirtingose finansų institucijose apskaičiuoti, taip įrodant pasiūlyto indekso praktinį pritaikomumą ir reikšmingumą (S3.1 lentelė).

S3.1 lentelė. Kibernetinio saugumo sričių ir rodiklių svorių nustatymas ir reitingavimas (sudaryta autorės)

Sritis	Rodiklis	Svoris	Rangas
Organizacinės priemonės	Kibernetinės rizikos vertinimas ir prioritetų nustatymas	0,07756917	1
Organizacinės priemonės	Investicijos į kibernetinio saugumo plėtrą	0,0770751	2
Incidentų valdymas	Veiksmų peržiūros ir testavimas	0,0736166	3
Organizacinės priemonės	Mokymai ir naudotojų švietimas	0,06818182	4

S3.1 lentelės pabaiga

Sritis	Rodiklis	Svoris	Rangas
Incidentų valdymas	Priemonės ir įrankiai, skirti pasekmėms mažinti	0,06175889	5
Organizacinės priemonės	Kibernetinės rizikos vidaus kontrolė	0,0583004	6
Techninės priemonės	Kibernetinių grėsmių, susijusių su galimais nuostoliais, vertinimas	0,05780632	7
Organizacinės priemonės	Atsakingo pareigūno (komandos) skyrimas	0,05731225	8
Incidentų valdymas	Atsigavimas po kibernetinio incidento	0,05632411	9
Techninės priemonės	Trečiųjų šalių atsakomybė už kibernetinį saugumą	0,05237154	10
Incidentų valdymas	Draudimas nuo kibernetinių rizikų	0,04594862	11
Techninės priemonės	Konkrečios saugumo sistemos	0,0444664	12
Teisinės priemonės	Pagrindinių atitikties rodiklių ataskaitos	0,04249012	13
Incidentų valdymas	Reagavimo į kibernetinius incidentus padalinys	0,04150198	14
Incidentų valdymas	Kibernetinių krizių valdymo planas	0,03754941	15
Teisinės priemonės	Įmonės vidaus politika ir (arba) gairės	0,03507905	16
Techninės priemonės	Prieiga prie neskelbtinų duomenų ir vidaus sistemų	0,02519763	17
Teisinės priemonės	Atitikties ir kibernetinio saugumo standartų užtikrinimas	0,02470356	18
Techninės priemonės	Galimų kibernetinių atakų motyvų nustatymas	0,01976285	19
Teisinės priemonės	Tarptautiniai teisiniai reikalavimai (ES lygmeniu)	0,01581028	20
Organizacinės priemonės	Strateginis požiūris į kibernetinę riziką	0,01531621	21
Incidentų valdymas	Pranešimo mechanizmas pažeidimo ir kibernetinės atakos atveju	0,01185771	22

Nagrinėjant ekspertų nuomones ir tyrimų rezultatus, patvirtinama, kad kibernetinės rizikos vertinimas ir prioritetų nustatymas yra svarbiausi kibernetinio saugumo veiksniai. Šie veiksmai padeda geriau suvokti atitinkamą riziką įmonei. Kadangi finansų įstaigos yra pagrindinis kibernetinių nusikaltėlių taikinys, galimų kibernetinių atakų spektras yra labai platus. Todėl, siekiant pagerinti kibernetinio saugumo lygį ir sumažinti kibernetinių išpuolių galimybę, rizikos prioritetų nustatymas tampa itin svarbiu veiksmu. Be to, įvairių kibernetinių atakų sukeliamos pasekmės turi įtakos įvairioms įmonės sritims. Jos gali padaryti žalos IT infrastruktūrai, lemti finansinius nuostolius, sutrikdyti veiklos tęstinumą ir sugadinti reputaciją.

Ekspertų nuomone, antrasis pagal svarbą kibernetinio saugumo rodiklis yra investicijos į kibernetinį saugumą. Kibernetinių atakų rūšys, kenkėjiški kodai ir

sukčiavimo atakos kasdien tobulėja, prisitaikydamos prie sparčiai besikeičiančios verslo aplinkos ir IT saugumo sprendimų. Metinko (2022) surinkti statistiniai duomenys įrodo, kad pasaulinės investicijos į kibernetinį saugumą kasmet ženkliai didėja ir 2023 m. jau sieks beveik 800 mlrd. Todėl finansų įstaigos turėtų nuolat investuoti į kibernetinio saugumo mokymus, kad sukurtų saugią verslo aplinką ir naujas priemones, kurios leistų išvengti kibernetinių atakų ar padėtų jas suvaldyti.

Trečiasis ir ketvirtasis rodikliai yra glaudžiai susiję tarpusavyje. Trečiasis yra veiksmų peržiūra ir testavimas, o ketvirtasis – mokymas ir naudotojų švietimas. Šis rezultatas rodo žmogiškojo veiksnio svarbą siekiant kibernetinio saugumo. Kaip įrodyta naujausiuose Georgiadou (2022) tyrimuose, atskirą kibernetinio saugumo dimensiją galima nurodyti atskiriems veiksniams, pavyzdžiui, požiūriui, sąmoningumui, elgsenai ir kompetencijai. Norint pagerinti visus šiuos kriterijus, būtina atidžiai peržiūrėti darbuotojų veiksmus, kai susiduriama su kibernetinio saugumo problemomis.

Šiame skyriuje aprašomas finansų įstaigų kibernetinio saugumo sudėtinio indekso sudarymo procesas ir rezultatai. Šie rezultatai grindžiami antrame skyriuje pateikta metodika. Sudėtinis kibernetinio saugumo indeksas (SKSI) apskaičiuojamas pagal šią formulę:

$$SKSI = \sum_{i=1}^{n} w_i I_{Ni}, \quad \text{(S3.1)}$$

čia: SKSI – sudėtinis kibernetinio saugumo indeksas; W_i – atitinkamas kibernetinio saugumo rodiklio I svoris; I_{Ni} – normalizuota kibernetinio saugumo rodiklio I reikšmė.

Čia pateikiama galutinė finansų institucijos sudėtinio kibernetinio saugumo indekso apskaičiavimo formulė:

$$\begin{aligned} SKSI = {} & 0{,}035\, I_1 + 0{,}016\, I_2 + 0{,}025\, I_3 + 0{,}042\, I_4 + 0{,}078\, I_5 + 0{,}058\, I_6 + 0{,}068\, I_7 + \\ & 0{,}077\, I_8 + 0{,}057\, I_9 + 0{,}015\, I_{10} + 0{,}058\, I_{11} + 0{,}044\, I_{12} + 0{,}052\, I_{13} + 0{,}020\, I_{14} + \\ & 0{,}025\, I_{15} + 0{,}046\, I_{16} + 0{,}012\, I_{17} + 0{,}074\, I_{18} + 0{,}042\, I_{19} + 0{,}038\, I_{20} + 0{,}062\, I_{21} + \\ & 0{,}056\, I_{22} \end{aligned} \quad \text{(S3.2)}$$

Šį pasiūlytą sudėtinį indeksą galima laikyti išsamia finansų institucijų kibernetinio saugumo vertinimo priemone, nes jį sudaro 4 pagrindinės kibernetinio saugumo sritys, 22 šių pagrindinių sričių rodikliai, apimantys svarbiausias problemas ir situacijas, konkretūs svoriai, nustatyti remiantis ekspertų vertinimu, ir vidaus vertinimo klausimynas, skirtas finansų institucijoms, kad būtų galima apskaičiuoti kiekvieno rodiklio individualius rezultatus. Vidinio vertinimo atlikimas yra labai svarbi šios vertinimo priemonės dalis, nes jame dalyvauja atstovai iš skirtingų organizacijos padalinių, atstovaujantys ne tik IT daliai, bet ir žmogiškiesiems ištekliams, strategijos įgyvendinimui, projektų valdymui. Apskaičiavus kiekvieno rodiklio rezultatus, institucija gali detaliai išanalizuoti savo kibernetinio saugumo ir kibernetinės rizikos valdymo praktiką. Klausimyno struktūra taip pat atkreipia dėmesį į galimus patobulinimus, nes joje pateikiami konkretūs teigiamų praktikų pavyzdžiai.

Naudodamos šią vertinimo priemonę finansų institucijos galėtų aprėpti ir įvertinti aktualias vidaus situacijas, atrasti rodiklius su mažiausiais balais, kurie yra jų reikšmingos silpnosios vietos, inicijuoti tam tikrus procesų ar investicijų pokyčius, susijusius su vertinimo rezultatais, ir tokiu atveju padidinti kibernetinio saugumo lygį. Skirtingai nuo kitų kibernetinės rizikos vertinimo priemonių indeksų, ši priemonė yra išskirtinė tuo, kad

yra orientuota būtent į finansų įstaigas. Kadangi priemonės teorinis pagrindas apima tokius elementus kaip jautrūs finansiniai duomenys ir atitinkami finansų institucijoms skirti teisiniai reglamentai, tai suteikia priemonei mokslinio naujumo ir didina jos praktinę vertę. Be to, atrinkti ekspertai, kurie atstovauja tik finansų institucijoms, vertino visus rodiklius, apibūdinančius kibernetinio saugumo sritis. Todėl rodiklių vertinimas ir rangavimas konkrečiai atspindi finansų institucijų aplinką ir problematiką.

Siūlomo sudėtinio finansų institucijos kibernetinio saugumo indekso aprobavimas buvo atliktas pagal metodiką, aprašytą antrajame skyriuje pateiktoje kibernetinio saugumo indekso sudarymo schemoje. Tyrimui atlikti buvo kreiptasi į tris skirtingų šalių (Lietuvos, Latvijos ir Estijos) finansų institucijas, kad jos, vadovaudamosi pasiūlytu modeliu ir indekso formule, pateiktų informaciją ir sudarytų savo kibernetinio saugumo indeksą. Toliau tekste finansų institucijos bus įvardytos taip: LTU1, LV2, EST3 (S3.2 lentelė).

S3.2.lentelė. Indekso rodiklių vertinimo rezultatai finansų institucijose LTU1, LV2, EST3 (sudaryta autorės)

Rodiklis	Svoris	Kodas	LTU1	LV2	EST3
Įmonės vidaus politika ir (arba) gairės	0,07756917	I_1	3	3	3
Tarptautiniai teisiniai reikalavimai (ES lygmeniu)	0,0770751	I2	5	5	5
Atitikties ir kibernetinio saugumo standartų užtikrinimas	0,0736166	I3	4	3	4
Pagrindinių atitikties rodiklių ataskaitos	0,06818182	I4	3	1	1
Kibernetinės rizikos vertinimas ir prioritetų nustatymas	0,06175889	I5	2	2	2
Vidaus kibernetinės rizikos kontrolė	0,0583004	I6	1	1	1
Mokymai ir naudotojų švietimas	0,05780632	I7	2	1	2
Investicijos į kibernetinio saugumo plėtrą	0,05731225	I8	2	1	1
Atskaitingo pareigūno skyrimas (komanda)	0,05632411	I9	2	1	2
Strateginis požiūris į kibernetinę riziką	0,05237154	I10	3	2	2
Kibernetinių grėsmių, susijusių su galimais nuostoliais, vertinimas	0,04594862	I11	2	2	2
Konkrečios saugumo sistemos	0,0444664	I12	3	2	2
Trečiųjų šalių atsakomybė už kibernetinį saugumą	0,04249012	I13	3	3	3
Galimų kibernetinių atakų motyvų nustatymas	0,04150198	I14	1	1	1
Prieiga prie neskelbtinų duomenų ir vidaus sistemų	0,03754941	I15	4	2	2
Draudimas nuo kibernetinių rizikų	0,03507905	I16	0	0	0
Pranešimo mechanizmas pažeidimo ir kibernetinės atakos atveju	0,02519763	I17	1	1	1

S3.2 lentelės pabaiga

Rodiklis	Svoris	Kodas	LTU1	LV2	EST3
Veiksmų peržiūros ir testavimas	0,02470356	I18	2	2	2
Reagavimo į kibernetinius incidentus padalinys	0,01976285	I19	1	1	1
Kibernetinių krizių valdymo planas	0,01581028	I20	1	1	1
Priemonės ir įrankiai, skirti pasekmėms mažinti	0,01531621	I21	1	1	1
Atsigavimas po kibernetinio incidento	0,01185771	I22	3	2	2

Kitas žingsnis pagal priimtą metodiką – surinktų verčių normalizavimas. Kadangi prieš apibendrinant duomenis juos reikia normalizuoti, tolesniems indeksų apskaičiavimams bus naudojami normalizuoti duomenys. Taip bus užtikrinta, kad apibendrinant būtų taikomi tie patys matavimo vienetai. Apskaičiuoti trijų finansinių institucijų kibernetinio saugumo indekso rezultatai pateikti S3.3 lentelėje.

S3.3 lentelė. Kibernetinio saugumo indeksas finansų institucijose LTU1, LV2, EST 3 (sudaryta autorės)

Finansinė institucija	Kibernetinio saugumo indeksas	Rangas
LTU1	0,41413	1
LV2	0,31838	3
EST3	0,34842	2

Atlikus galutinius kibernetinio saugumo indekso skaičiavimus trijose konkrečiose finansų įstaigose, pateikiamos prielaidos ir rezultatų vertinimas. Analizuojant rezultatus pagal šalis, aiškiai matyti, kad kibernetinio saugumo lygis visose šalyse yra žemesnis nei 0,5 punkto. Aukščiausia reikšmė yra Lietuvoje, žemiausia – Latvijoje. Analizuojant skaičiavimo rezultatų detales, svarbu atkreipti dėmesį į rodiklių svorius ir juose pasiektus balus. Svarbiausiu kibernetinio saugumo rodikliu buvo pasirinktas „reguliarus rizikos vertinimas ir prioritetų nustatymas“. Visos trys įmonės šioje srityje surinko tik pusę balų (2 iš 4), o tai reiškia, kad įmonės tik kartą per metus peržiūri rizikos vertinimo dokumentus ir nustato prioritetus. Atsižvelgiant į sparčiai besikeičiančią verslo ir saugumo aplinką, tokį dažnį reikėtų laikyti nepakankamai dažnu.

Aptariant investicijas į kibernetinį saugumą (kas taip pat buvo tarp ekspertų pasirinktų 5 geriausių rodiklių), visos trys institucijos nepasiekė aukštų verčių. Tai reiškia, kad įmonės į kibernetinio saugumo plėtrą investuoja mažiau nei 5 proc. savo apyvartos. Palyginti su JAV verslo aplinka ar net kai kuriomis ES šalimis, šis investicijų rodiklis yra mažas, turint omenyje, kad finansų institucijose kibernetinė rizika yra viena iš aktualiausių.

Tarp svarbiausių rodiklių buvo veiksmų peržiūra ir testavimas. Visos trys įmonės šioje srityje surinko maksimalų balų skaičių, o tai reiškia, kad įmonės nuolat vykdo sistemų ir darbuotojų testavimo procesą ir vertina jų veiksmus bei žinias, susijusias su kibernetiniu saugumu.

Viena iš *sudėtinio kibernetinio saugumo indekso* funkcijų ir panaudojimo galimybių – nustatyti įstaigos pažeidžiamumą ir silpnąsias vietas. Atlikus vidinį kibernetinio saugumo vertinimą remiantis sukurtu vidinio įsivertinimo klausimynu, mažiausias vertes surinkę rodikliai gali būti identifikuojami kaip esminės pažeidžiamos vietos, į kurias reikėtų atkreipti dėmesį siekiant padidinti kibernetinio saugumo lygį.

Bendrosios išvados

1. Atlikta literatūros analizė patvirtina, kad kibernetinis saugumas tampa vis didesne verslo rizika, galinčia turėti įtakos verslo tęstinumui, reputacijai ir pelningumui. Kibernetinės rizikos ir saugumo lygio vertinimas yra sudėtingas, tačiau labai svarbus procesas. Mokslinės literatūros apžvalga rodo, kad kibernetinių atakų poveikis skiriasi priklausomai nuo kibernetinės rizikos rūšies. Atsižvelgiant į kibernetinės rizikos klasifikavimo metodų įvairovę, kibernetinių rizikų analizė yra labai svarbi įgyvendinant rizikos vertinimo strategijas ir pasirengimo priemones bei įvertinant galimas išlaidas, susijusias su kibernetinėmis rizikomis.
2. Finansų institucijos pripažįstamos itin svarbiais ir labai pažeidžiamais subjektais kibernetinio saugumo srityje visų pirma dėl to, kad jos saugo ir naudoja daug jautrių duomenų. Mokslinėje literatūroje pabrėžiama, kad finansų institucijoms, atsižvelgiant į jų valdomos informacijos apimtį, kyla didesnė kibernetinė rizika. Dėl finansinių paslaugų pobūdžio finansinės institucijos tampa pagrindiniais kibernetinių įsilaužėlių taikiniais. Išnagrinėtuose moksliniuose tyrimuose teigiama, kad siekdamos suteikti saugias finansines paslaugas ir laikytis teisinių reglamentų finansų institucijos turi aktyviai dalyvauti kibernetinės rizikos vertinimo procesuose.
3. Atlikus išsamią kibernetinės rizikos ir kibernetinio saugumo sudedamųjų dalių struktūros ir ypatumų analizę, nustatytos keturios pagrindinės finansų institucijų kibernetinio saugumo sritys: teisinės priemonės, organizacinės priemonės, techninės priemonės ir incidentų bei krizių valdymas. Atliekant interviu su ekspertais ir taikant MCDM metodus buvo nustatyti 22 kibernetinio saugumo rodikliai (4 teisinės srities rodikliai, 6 organizacinės srities rodikliai, 5 techninės srities rodikliai ir 7 incidentų valdymo srities rodikliai.
4. Sukurta kibernetinio saugumo vertinimo priemonės kūrimo metodika, kurią sudaro 4 pagrindinės kibernetinio saugumo sritys, 22 rodikliai, ekspertų nustatyti individualūs kiekvieno rodiklio svoriai, išreiškiantys jų svarbą bendrame kibernetinio saugumo kontekste, ir klausimynas, skirtas kiekvieno rodiklio vidiniam vertinimui finansų institucijoje.
5. Tolesniems tyrimams ir sudėtiniam indeksui sudaryti buvo pasirinkti šie tinkamiausi metodai: daugiakriterinių sprendimų priėmimo metodai (SAW ir TOPSIS), skirti ekspertų vertinimų duomenims apdoroti, ir OECD metodika, tinkama sudėtiniam indeksui sudaryti.
6. Atlikus daugiakriterinį ekspertinį vertinimą ir pasinaudojus TOPSIS metodu, buvo nustatyta, kad *duomenų saugumas* yra didžiausia prioritetinė rizika finansų

institucijose. Duomenų saugumas yra svarbus, nes apsaugo komercinius ir finansinius duomenis bei jautrią ir privačią klientų informaciją.

7. Kibernetinio saugumo rodikliai buvo reitinguojami atlikus ekspertų apklausas ir taikant daugiakriterinės sprendimų priėmimo analizės metodą SAW apdorojus jų rezultatus. Svarbiausiu rodikliu buvo pasirinktas *kibernetinės rizikos vertinimas ir prioritetų nustatymas*, antruoju svarbiausiu – *investicijos į kibernetinio saugumo plėtrą*, trečiuoju – *veiksmų peržiūros ir testavimas*.
8. Sukurtas sudėtinis kibernetinio saugumo indeksas, kuris leidžia finansų institucijai, atlikus vidinį vertinimą, nustatyti bendrą kibernetinio saugumo lygį ir problemines sritis. Sudėtinis kibernetinio saugumo indeksas leidžia išsamiai išanalizuoti silpnąsias kibernetinio saugumo sritis, taip pat nustatyti priemones, kurių galima imtis kibernetinio saugumo lygiui pagerinti.
9. Sudėtinis kibernetinio saugumo indeksas buvo praktiškai pritaikytas individualiai įvertinant trijų skirtingų finansų institucijų kibernetinio saugumo lygį. Šis praktinis vertinimas leido išbandyti sukurtą priemonę ir palyginti skirtingų institucijų rezultatus. Todėl ši priemonė gali būti naudojama ne tik kaip vidinio vertinimo priemonė, bet ir kaip bendras rodiklis finansų sektoriaus kibernetinio saugumo lygiui palyginti ir įvertinti.

Tyrimo apribojimai ir būsimų tyrimų kryptys

Atliktam tyrimui taikomi šie apribojimai:

1. Tyrime daugiausia dėmesio skiriama konkrečių Baltijos šalių (Lietuvos, Latvijos ir Estijos) finansų įstaigoms. Tyrimo rezultatai gali būti netaikomi visuotinai, o kibernetinio saugumo situacija skirtinguose regionuose ir skirtingų tipų finansų įstaigose gali labai skirtis.
2. Tyrime užfiksuota trumpalaikė kibernetinio saugumo praktikos apžvalga konkrečiu metu. Dinamiškas ir kintantis kibernetinio saugumo grėsmių pobūdis reiškia, kad priemonių veiksmingumas laikui bėgant gali keistis, todėl išvadas būtina atnaujinti ir atnaujinti kai kurias detales.
3. Tyrime daugiausia dėmesio skiriama konkrečiam rodiklių rinkiniui, todėl kai kurie svarbiausi kibernetinio saugumo aspektai gali būti tinkamai neaptarti. Pavyzdžiui, tyrimo apimtį gali apriboti tai, kad išsamiai nenagrinėjamos naujos technologijos, pavyzdžiui, dirbtinis intelektas kibernetinio saugumo srityje.

Galimos tolesnio darbo kryptys:

1. Atliekant ilgesnio laikotarpio longitudinius tyrimus, būtų galima gauti įžvalgų apie kibernetinio saugumo priemonių veiksmingumą laikui bėgant. Tai padėtų suprasti grėsmių raidą ir saugumo priemonių pritaikomumą.
2. Tyrimų išplėtimas įtraukiant ne tik finansų įstaigas, bet ir įvairias pramonės šakas, leistų tyrėjams palyginti kibernetinio saugumo praktiką įvairiuose sektoriuose. Ši lyginamoji analizė galėtų išryškinti konkrečioms pramonės šakoms būdingus iššūkius ir geriausią praktiką.

3. Tyrimo išplėtimas įtraukiant įvairesnes šalis ir regionus padėtų išsamiau suprasti pasaulinę kibernetinio saugumo praktiką. Tai galėtų atskleisti regioninius skirtumus ir išryškinti bendrus iššūkius, su kuriais susiduria organizacijos visame pasaulyje.
4. Ateityje atliekant tyrimą būtų galima nagrinėti reagavimo į incidentus mechanizmus, analizuojant, kaip organizacijos elgiasi su kibernetinio saugumo incidentais ir atsigauna po jų. Reagavimo į incidentus planų veiksmingumo supratimas yra labai svarbus siekiant padidinti bendrą kibernetinio saugumo atsparumą.
5. Šių trūkumų pašalinimas ir šių būsimų tyrimų krypčių nagrinėjimas padėtų išsamiau ir visapusiškiau suprasti kibernetinio saugumo praktiką finansų įstaigose.

Julija GAVENAITĖ-SIRVYDIENĖ

DEVELOPMENT OF CYBER SECURITY ASSESSMENT TOOL FOR FINANCIAL INSTITUTIONS

Doctoral Dissertation

Social Sciences,
Economics (S 004)

KIBERNETINIO SAUGUMO VERTINIMO PRIEMONĖS SUKŪRIMAS FINANSŲ INSTITUCIJOMS

Daktaro disertacija

Socialiniai mokslai,
Ekonomika (S 004)

Lietuvių kalbos redaktorė Aušra Kundrotaitė
Anglų kalbos redaktorė Jūratė Griškėnaitė

2024 04 30. 13,3 sp. l. Tiražas 20 egz.
Leidinio el. versija *https://doi.org/10.20334/2024-023-M*
Vilniaus Gedimino technikos universitetas
Saulėtekio al. 11, 10223 Vilnius
Spausdino UAB „Ciklonas“,
Žirmūnų g. 68, 09124 Vilnius