

Data-Driven Evaluation of Cybersecurity Costs in The Digital Era: Managerial Implications for IT Companies

Algita Miečinskienė, Alina Bespalova

Department of Financial Engineering, Faculty of Business Management, Vilnius Gediminas Technical University, Saulėtekio al. 11, LT-10223 Vilnius, Lithuania

algita.miecinskiene@vilniustech.lt (Corresponding author)

Received date: Oct 20, 2025, revision date: Nov. 29, 2025, Accepted: Dec. 18, 2025

ABSTRACT

In the digital era, cybersecurity has become a critical managerial concern for IT companies, as cyber risks increasingly affect financial performance, operational continuity, and strategic decision-making. This study proposes a data-driven approach to evaluating and managing cybersecurity costs by integrating cyber risk forecasting with multi-criteria decision analysis. Using the Global Cost of Cyber Risk Calculator and firm-level proportional estimation, the study forecasts potential cyber-attack losses for the Lithuanian IT sector and a representative IT company over the period 2025–2029. Survey data from IT and finance managers are further analysed using the TOPSIS method to prioritise cybersecurity investment strategies. The results indicate a substantial growth in projected cyber-attack costs, highlighting the need for proactive and structured cybersecurity investment decisions. Among alternative measures, advanced firewall and intrusion detection systems, secure network architecture, and employee training emerge as the most effective strategies for reducing cyber risk exposure. This study contributes to the literature on management changes in the digital era by demonstrating how data-driven risk assessment tools can support managerial decision-making in cybersecurity investment. Practically, the findings provide IT managers with a structured framework for allocating cybersecurity resources more effectively in the face of increasing digital uncertainty.

Keywords: cybersecurity, cyber risk management, cybersecurity cost, cybersecurity measures, firewall, intrusion detection systems, cyber-attacks, IT security.

1. Introduction

Institutions of various sizes, business types, or locations around the world have increasingly been affected by the consequences of cyberattacks, impacting financial, operational, reputational, and other areas. Over the past few years, the financial sector has witnessed a significant rise in cyber risk exposure. Although cybersecurity and business resilience have improved, attackers continue to evolve their techniques, shifting their key targets and adapting their models of cyberattacks. Financial institutions, as prime targets, are particularly vulnerable due to their reliance on technology and digital platforms.

Organisations are faced with a constantly evolving risk landscape. This has led to new challenges, including more complex and expensive business interruptions, an increase in the frequency and cost of cyberattacks, significant consequences from large-scale data breaches, and stricter regulations. As many companies transitioned to remote work, cybercriminals have been exploiting new vulnerabilities to access private databases, sensitive information, and internal networks. Human error or IT disruptions have also become significant indicators of cyber risks.

In this environment, financial institutions, which hold vast amounts of sensitive data and financial resources, are under growing pressure from increasingly sophisticated cyber-attacks. These risks come in various forms, and in a changed business landscape, they are harder to predict and identify. The primary reason for the importance of cybersecurity is to safeguard customer data, financial assets, business continuity, and internal

resources. Therefore, institutions must implement robust cybersecurity programs, take preventive measures, and plan cybersecurity investments. The potential consequences of cyber-attacks, such as personal data breaches or financial credential leaks, could not only damage a company’s reputation but also threaten its financial stability and business continuity.

Cyber-attacks have caused significant financial and non-financial losses due to their increasing frequency and costs. Developing accurate forecasts of cyber losses can be a valuable tool for companies to evaluate their preparedness, invest in cybersecurity, and prevent business disruptions.

The purpose of this research is to forecast the potential financial costs that cyber-attacks could impose on IT companies, utilising advanced risk assessment models.

Research methodology: To achieve this aim and prepare a forecast of cyber-attack costs, the study used the Estimation of the Global Costs of Cyber Risk Calculator V 1.2 tool, the TOPSIS multi-criteria decision analysis (MCDA) method, as well as methods such as comparative data analysis, data modelling, and statistical analysis.

This paper consists of three main parts. The theoretical part is dedicated to a systematic review of the concept of cybersecurity, discussing various approaches proposed by researchers and outlining key issues in the field of cybersecurity. The methodology part describes and explains the methodology for estimating cybersecurity costs. The last part presents the results of the cyber cost evaluations, offering conclusions and a discussion on the topic.

2. Cyber Risk Concept Analysis

Cyber risk is increasingly recognised as a complex and evolving challenge that affects not only technical systems but also organisational processes, human factors, and the broader digital ecosystem. Identifying and mitigating these risks requires continuous evaluation and adaptation to the ever-changing cyber landscape. As cyber-attacks grow in sophistication, businesses and governments must adopt robust risk management frameworks to safeguard critical resources and ensure operational resilience (Liu et al., 2022). Cyber risk is defined as the potential adverse consequences resulting from unauthorised access, manipulation, or destruction of information systems. This definition emphasises the importance of adopting standardised risk management practices to facilitate better communication and coordination among stakeholders (Cremer et al., 2022). As a result, proactive and adaptive risk management strategies are crucial for effectively countering these threats. The concept of cyber resilience has gained prominence, requiring organisations to adopt both reactive defences and proactive measures to develop adaptive capabilities that withstand and recover from cyber incidents (Odeyar et al., 2025). Organisations must move beyond traditional defences and develop flexible strategies that enable them to anticipate, mitigate, and recover from attacks (Fauzi et al., 2023).

Table 1 below summarises recent descriptions of cyber risk from academic literature, reflecting the multifaceted nature of cyber threats.

Table 1: Definition of cyber risk

Authors	Cyber Risk Description Summary
Howell et. al. (2025)	Cyber risk refers to the dangers associated with the use of information and communication technologies (ICT), stemming from criminal activities, technological failures, and evolving cyber threats.

Authors	Cyber Risk Description Summary
Cremer et. al. (2022)	Cyber risk refers to disruptions in information systems, requiring comprehensive and standardised management strategies.
Odeyar, 2025	Cyber risk is an inevitable occurrence, emphasising ongoing challenges. It requires a proactive strategy that focuses on adaptive capabilities and reactive responses.
Fauzi et al. (2023)	Cyber risk encompasses organisational, human, and digital vulnerabilities, necessitating holistic and interdisciplinary approaches.
Liu et al., 2022	Cyber risk is a dynamic and complex concept that is critical to cybersecurity and risk management. It demands thorough investigation for flexible and resilient plans, addressing the ever-changing threats in cyberspace.

From a national security perspective, cyber risks are among the most significant threats, with the potential for catastrophic financial and geopolitical consequences. Cyber-attacks on critical infrastructure, military systems, and key economic sectors expose significant vulnerabilities, with potential consequences for financial stability, privacy, and geopolitical relations (Cremer et al., 2022). The growing interdependencies in cyberspace demand international collaboration to mitigate the risks posed by state-sponsored cyber-attacks and other large-scale cyber threats (Yarovenko, 2020). In addition to compromising financial stability, unauthorised access to private data and critical infrastructure can damage organisational reputations and erode stakeholder trust, highlighting the importance of robust cybersecurity measures (Sharma, 2024).

Cyber risk classifications play a crucial role in identifying, measuring, modelling, and managing cyber risk events, providing structured frameworks to understand and categorise different types of cyber threats (Malavasi et al., 2026). Some of the most concerning types of cyber risks include social engineering attacks, such as phishing, which exploit human error to bypass security protocols. Phishing remains a key entry point for more severe attacks, such as ransomware, which encrypts sensitive data and demands payment for its release (Ilany-Tzur & Fink, 2025). Ransomware continues to impose significant financial and operational burdens on organisations, often leading to business disruptions and reputational damage (Fotis, 2024). Other notable cyber threats include distributed denial-of-service (DDoS) attacks, which overwhelm systems and shut down critical services, and insider threats, where trusted individuals exploit their access to cause harm (Ouhssini et. al., 2024).

Table 2 summarises different types of cyber threats from the literature, reflecting their varied impacts on organisations.

Table 2: Cyber threat types described

Threat Type	Description	Implications	Scientific Reference
Malware	Malware, short for malicious software, is a term that encompasses various types of software designed to infiltrate, damage, or exploit computer systems without the owner's consent. It can perform a range of harmful activities, including stealing, encrypting, modifying, or deleting data, as well as monitoring user activities.	Financial losses, intellectual property theft, business disruption, data breaches, and reputational harm.	Ji & Mogos, 2025; Solfa, 2022
Phishing	A form of social engineering using fake emails, messages, or websites to trick victims into disclosing private information.	Identity theft, unauthorised access, monetary losses, compromised data security, and psychological effects.	Ilany-Tzur & Fink, 2025; Qasaimeh & Jaradeh, 2022; Sharma, 2024
DDoS Attacks	Distributed denial-of-service attacks overload a target system.	Financial losses, paralysed e-commerce platforms, disrupted online services, and damaged reputation.	Ouhssini et al., 2024; Jeyavim & Parkavi, 2025
Insider Threats	Threats from individuals associated with an organisation.	Monetary losses, security lapses, intellectual property theft, data leaks, and reputational harm.	Inayat et al., 2025; Randive et al., 2023
Advanced Persistent Threats (APTs)	Well-planned and sophisticated cyberattacks aim for unauthorised access to vital systems.	Compromised sensitive data, intellectual property theft, espionage, and broader geopolitical ramifications.	Alshamrani et al., 2019; Eisenbach et al., 2021; Ghelani et al., 2022

The increasing sophistication of cyber threats underscores the need for organisations to adopt comprehensive, multi-layered defence strategies. This involves not only technical solutions, such as firewalls, intrusion detection systems, and encryption, but also policy-driven measures, continuous employee training, and the development of a resilient cybersecurity culture. Proactive collaboration across sectors and international partnerships is crucial for addressing the interconnected risks posed by modern cyber threats.

3. Research Design and Methodology

3.1. Research framework

As the threat landscape of cyberattacks continues to evolve within the financial sector, there is a growing need for robust methods to estimate both the current and potential future costs of cyber risks and use the best measures to minimise them. This research employs several analytical techniques to assess the potential impact of cyber hazards on Lithuania's IT industry, with a focus on a specific IT company. Figure 1 outlines the methodological framework for this study.

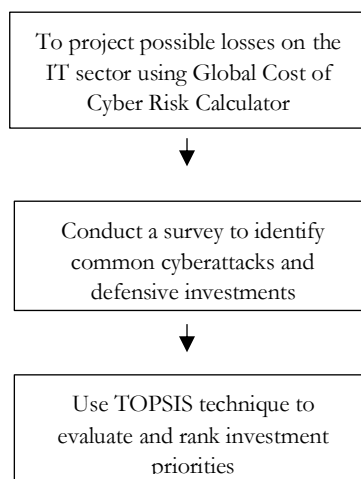


Figure 1: Methodology scheme for the Evaluation of Cybersecurity Costs (Source: designed by authors)

In the first stage, the Global Cost of Cyber Risk Calculator is used to project possible losses to Lithuania's IT industry between 2025 and 2029. The research incorporates real-world data to assess the projected impact of cyberattacks, playing a critical role in forecasting the potential damage caused by these attacks in the IT sector.

It involves obtaining detailed financial information from reputable sources, such as Bloomberg, Reuters, and Yahoo Finance. Numerous financial variables, including stock prices, market movements, corporate financial statements, and economic indicators, are among the data gathered. This stage ensures that the analysis is based on accurate and current data, providing a solid foundation for the subsequent stages, as outlined by Dreyer et al. (2018). Using models and algorithms, the calculator assesses the potential impact of cyber threats on financial institutions. The proposed methodology integrates several factors, including incident frequency, financial hazards, and systemic implications, to provide a flexible and adaptable framework for assessing the cost of cyber risk. The methodology first determines the value at risk by country and industry sector, then offers insights into the potential financial consequences of cyber catastrophes. This technique considers factors such as industry resilience and regional vulnerabilities in order to carefully analyse the potential severity of cyberattacks and the ensuing economic consequences. Organisations can gain a better understanding of their vulnerability and prioritise investments in cybersecurity solutions by evaluating the financial impact of cyber hazards.

In the second stage, experts from financial and IT departments within Lithuanian financial sector companies participated in a survey to identify the most prevalent cyberattacks and the types of preventative measures currently being considered. The survey includes questions about the types and frequency of cyberattacks, such as ransomware, phishing, malware, and DDoS attacks. Additionally, it enquires about the cybersecurity investments and methods that have been made, such as incident response plans, firewalls, antivirus software, intrusion detection systems, and employee training initiatives.

To determine cybersecurity investment priorities, the "Technique for Order of Preference by Similarity to Ideal Solution" (TOPSIS) was applied. This multi-criterion decision-making methodology evaluates measures by weighing anticipated damage (results provided by the "Global Cost of Cyber Risk Calculator") and investment costs, providing the best cyber risk management measure.

Therefore, the methodology provides stakeholders and company leaders with robust tools and methods for comprehensive evaluation of cyber risk. By leveraging transparent and scalable frameworks such as TOPSIS, decision-makers can efficiently allocate resources and develop informed measures to mitigate cyber threats,

ensuring organisational resilience and safeguarding the financial sector against a rapidly growing threat landscape.

3.2. Cyber risk cost forecasting approach

The developed model makes it possible to assess how different cyberattacks affect the GDP (gross domestic product) of businesses in the area. To build this model, the following conditions must be specified (Dreyer et al., 2018):

1. Nations: $c \in C$.
2. Sectors of the industry: $i \in I$.
3. Exposures to the economy: $e \in E$.
4. Dangers: $p \in P$.

The model's structure includes a dimension of countries C , industry sectors I , economic exposures E , and hazards P . All countries c belong to the C country dimension, industry sectors i to the I industry sectors dimension, financial exposures e to the economic exposures E dimension, and hazards p to the P perils dimension. Since dimensions are used to define things, they cannot be divided (Dreyer et al., 2018).

Although each dimension is said to constitute a significant component of the others, they may not be mutually exclusive or all-inclusive. For example, the value of the dimension of nations C , which is a sub-dimension of all countries worldwide, is contingent upon the accessibility of information. It is also possible to characterise the dimension of industry sectors I as comprehensive or incompatible. Therefore, it is suggested that the dimensions of financial exposures (E) and hazards (P) are mutually exclusive as well as collectively exhaustive. Given the frequency of cyberattacks, it is possible that these dimensions will expand beyond what is currently described by this methodology. Additionally, the model's creators assumed additive segregation of direct costs, meaning that when predicting direct expenses, sub-dimensions within each dimension associate with estimates of wider systemic expenditures rather than having an impact on one another (Jacobs et al., 2017).

The technique investigation connects cyberattack losses to GDP losses in a particular industry and sector. This method provides for both rebound effects between organisations (where damage in one organisation may lead to a benefit in another organisation) and lessens the need to compute over a variety of vastly unclear forms of damages.

The costs are specifically broken down as follows (Dreyer et al., 2018):

- output damages, which are handled by all sectors in all countries c ;
- the macroeconomic effects on production that are accepted by all sectors as a result of the direct expenditures by all sectors in all countries c .

Within this framework, direct costs are those that an industry must bear entirely at any one time during a cyber-risk event. These expenditures consist of attestation setup fees, fines, costs related to raids and investigations, and company closures that take place in the sector that was the focus of the cyberattack. They also consist of prospective legal fees that third parties might suffer but are paid for by the company that was attacked online.

By adding the dimensions (c , i , e , and p) to G_c , which is the GDP of the nation, the model calculates the GDP and immediate costs of exposure for each sector i inside country c . The subsequent steps are performed (Dreyer et al., 2018):

1. w_{ci} is defined as sector i 's shares of GDP in country c .

2. $w_{ci} * G_c$ is the value added (contribution to GDP) of sector i in country c .
3. it is also defined O_{ci} as the sector output of sector i in country c .
4. the unitless value Y_{cie} is described as the fraction of industry sector output that is adequate to the amount of money at risk from every exposure type (e), despite of whether they can be affected by a cyber-attack.
5. definition of unitless value X_{ciep} follows to be the fraction of the outcome at risk in country (c), industry sector (i), and exposure type (e) that will be completely demolished, stolen, or otherwise lost due to a specific peril (p).
6. the merger of Y_{cie} and X_{ciep} 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 .

The immediate cost to sector exposure in each sector i in nation c can be computed by adding the product Y_{cie} and X_{ciep} for all dangers p and results e , based on the measurements and linkages provided. The overall sector direct costs to exposures can then be obtained by multiplying this sum by the sector i in nation c (O_{ci}) (Drayer et al., 2018):

$$d_{cio} = o_{ci} \sum_{e \in E}^1 \times \sum_{p \in P} Y_{cie} + X_{ciep} \quad (1)$$

Allowing direct costs (d) to represent the loss to sector GDP and accounting for any modifications in the sector exposure scale to changes in sector GDP allows one to closely express the direct exposures to sector GDP (Drayer et al., 2018):

$$d_{cig} = w_{ci} G_c \sum_{e \in E} \sum_{p \in P} Y_{cie} X_{ciep} = \frac{w_{ci} G_c}{O_{ci}} d_{cio} \forall i \in I, c \in C \quad (2)$$

Additionally, we can evaluate each nation's GDP and total direct costs of exposure to cyber risks by aggregating sector-level direct costs (d), as explained below (Drayer et al., 2018):

$$d_{co} = \sum_{i \in I} d_{cio} \text{ and } d_{cg} = \sum_{i \in I} d_{cig} \forall c \in C \quad (3)$$

The GDP of country c in sector i is a commonly accepted value. Because of the volatility and density of sets in cyber-risk assessments, it may be beneficial to evaluate the effects of various techniques on this value. The risks, exposures, industries, and combinations of these inputs may have a substantial impact on how the outcome is evaluated. As such, it is very difficult to determine how dangers affect exposures, even though identifying sectors and exposures is simple.

For the calculator to forecast, it needs to be provided with multiple distinct sets of dimensions. Dimension sets were estimated utilising information from studies and research conducted by scientists in order to verify the estimates. Dimensions can be point assessments or potential results that are then combined to provide exposure circulations and estimated values (Drayer et al., 2018):

1. Country (C) – consider that c is defined as a specific country inside a dimension of countries called C. This dimension is expanded to include countries that are becoming increasingly vulnerable. The connection between countries and sectors allows for a comprehensive analysis of how industries correspond with countries. The approach utilises OECD-collected financial and accessible data.
2. Industry sectors (I) – authors identified the most significant industries for cyber-risks by segmenting the economy based on available country-level data. The Structural Analysis Database serves as the foundation for country-level economic information.
3. Financial exposure (E) – e is defined as a financial exposure that could be harmed, regardless of the danger type. These exposures, as an input to production, that, if harmed by a cyber assault, can affect a firm's overall income, rather than directly contributing to GDP. Also, financial exposures are defined as capital assets, intellectual property (IP), and income, as described. To assess the value of assets and intellectual property, we take into account the associated output. This allows us to think of it as a percentage of GDP, which is a flow variable.
4. Capital assets – refer to a company's tangible property, including land, buildings, machinery, vehicles, and computers. Cyber dangers have the potential to negatively impact capital assets and lower income, making them a financial risk for the organisation.

Summarising, the “Global Cost of Cyber Risk Calculator” provides a model for evaluating current and future financial losses from cyberattacks in the financial sector. It considers factors such as event frequency, unpredictability, and diverse sources of cyber threats. The calculator estimates value at risk by analysing financial exposures and computes both direct costs (e.g., financial losses and recovery expenses) and systemic costs (e.g., broader economic impacts). By incorporating probability distributions and modelling tools, it forecasts potential damages to the financial sector, offering clear insights to support strategic planning and resource allocation for risk management.

3.3. Decision-support method (TOPSIS)

A proportionate calculation method is used to quantify the possible harm unique to the IT company. The expected harm is determined by multiplying the total cybersecurity damage predicted for each year by the ratio of the specific IT company's revenue to the entire revenue of Lithuania's IT sector. The cybersecurity damage for a particular company of IT is projected using this proportional strategy over the same five-year timeframe, 2025–2029:

$$\frac{\text{Revenue of the company}}{\text{Revenue of the business sector}} \times \text{Business sector cybersecurity damage} = \text{Company's cybersecurity damage}$$

The employees of the IT company's IT and financial departments participated in a survey to determine which cyberattacks are most common and to gather information about anticipated investments in defence strategies. The poll also gathers data regarding the many kinds of preventative strategies under consideration.

Using the Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) technique, the most effective preventive strategy for an IT company is identified. Using an anticipated harm and predicted investment, this multi-criteria decision-making methodology assesses the effectiveness of the proposed preventive measures (Shih, 2022). By ranking the preventative techniques, the TOPSIS method makes it possible to determine the best course of action for reducing cyber risks at an IT company.

The Technique for Order Preference by Similarity to Ideal Solution (TOPSIS), first presented by Hwang and Yoon in 1981, has gained widespread recognition as a key paradigm in decision-making techniques. The fundamental notion of TOPSIS is to find the alternative that, when expressed in geometric distance, minimises its distance from the positive ideal solution and maximises its distance from the negative ideal

solution. Using this approach, TOPSIS assigns a ranking to each alternative according to how close it is to the positive ideal solution and how far it is from the negative ideal solution (Shih, 2022).

As described by Velasquez, the TOPSIS process consists of the following crucial steps (Shih, 2022):

- **Normalisation:** To guarantee that every criterion is on the same scale and of equal importance, normalise the decision matrix.
- **Weight Assignment:** Give each criterion a weight according to how important it is to the decision-making process.
- **Determination of Positive and Negative Ideal Solutions:** Determine the greatest and worst possible outcomes, respectively, for each criterion by identifying the ideal and anti-ideal solutions.
- **Distance Calculation:** Determine the separations between the positive and negative ideal solutions and each option.
- **Similarity Calculation:** Determine how similar each option is to the positive and negative ideal solutions by calculating its similarity scores.
- **Ranking:** Sort the options according to how comparable they are, with higher scores denoting superior functionality.

Through the use of TOPSIS, decision-makers can effectively assess and rank options in a methodical manner, resulting in well-reasoned choices in intricate decision-making situations.

4. Results

4.1. Forecasted cyber risk costs

This study uses the Global Cost of Cyber Risk Calculator to forecast the potential financial damage from cyber-attacks in Lithuania's IT sector, with a focus on a prominent IT company named S. The projected damage from cyberattacks on Lithuania's IT sector for the years 2025–2029 is shown in the first chart (Figure 1) and is stated in millions of euros. Over the next five years, the damage is expected to climb steadily, according to this forecast. According to the analysis, sector-wide damages are expected to grow by 64 % from €16.22 million in 2025 to €26.57 million in 2029.

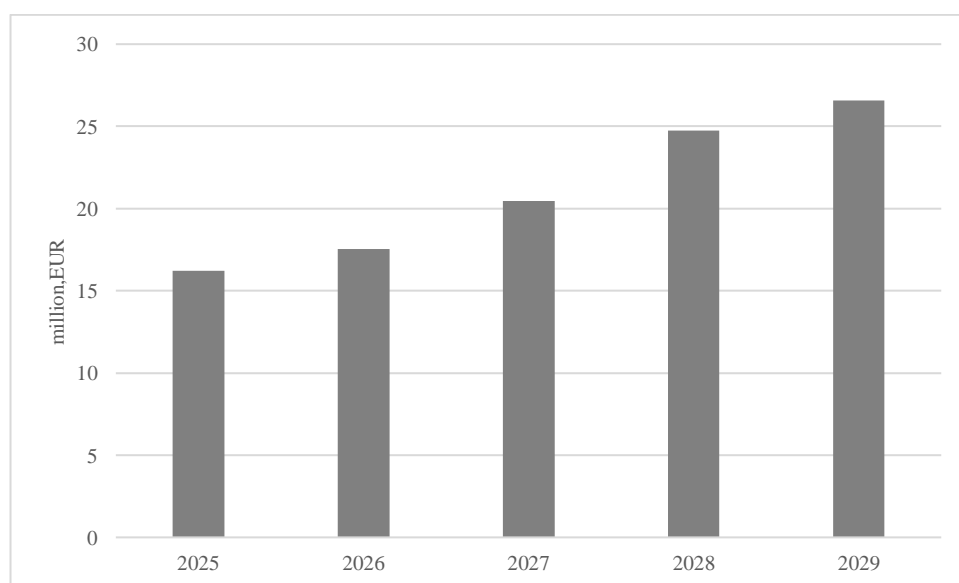


Figure 1: Forecasted costs of cyber-attacks by 2025-2029 within the IT sector in Lithuania (million, EUR) (source: compiled by authors using Global Cost of Cyber Risk Calculator V 1.2)

The projected damage from cyberattacks against the IT company for the same time is shown in the second chart (Figure 2) and is again indicated in millions of euros. For the IT company, the forecasted damage is projected to increase by 64.4 % over the same period, starting from €2.08 million in 2025 and rising to €3.42 million in 2029.

According to this estimate, the IT company is forecasted to have about 12 % harm in the overall IT industry, but the damage is increasing steadily over the next five years. This illustrates the proportionate computation based on the IT company's revenue in relation to the total revenue of the IT industry in Lithuania.

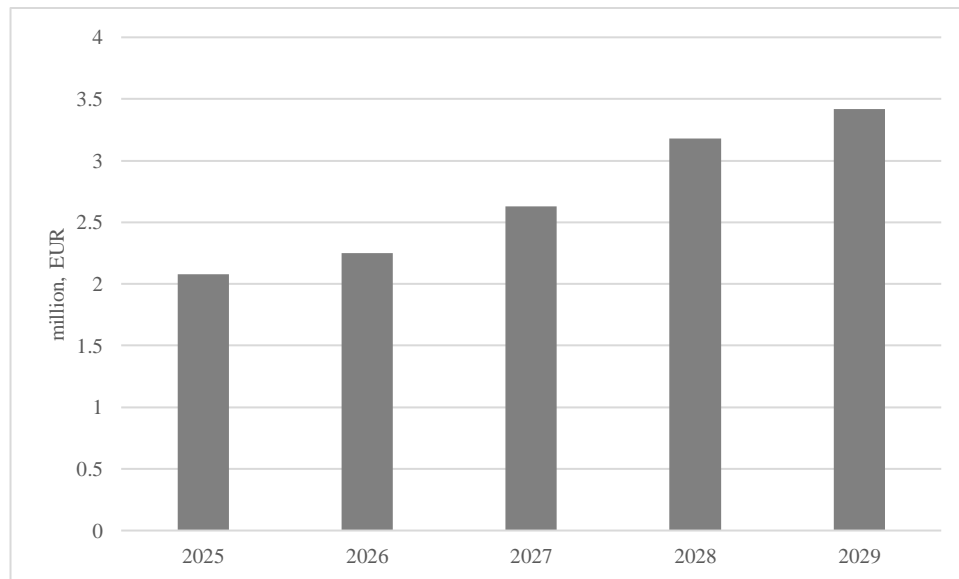


Figure 2: Forecasted costs of cyber-attacks by 2025-2029 within the UAB S. (million, EUR) (source: compiled by authors)

All things considered, both charts (Figures 1 and 2) show that the threat of cyberattacks is growing for the IT company as well as in the IT industry in Lithuania, highlighting the importance of investing in efficient cybersecurity solutions to mitigate these rising threats. These figures highlight the escalating financial impact of cyber threats and emphasise the necessity of robust cybersecurity investments.

4.2. Cyber threat profile and investment priorities

This research examines the survey data, highlighting key findings and their implications for enhancing the organisation's cybersecurity resilience. To find out more about the cyber threats that the IT company confronts, the finance and IT departments took part in a survey (10 people). Respondents were asked to identify the most common types of cyberattacks they encountered in their work environment. The most frequent types of cyberattacks reported by respondents were as follows:

1. Phishing attacks (40 % of respondents);
2. Ransomware (35 % of respondents);
3. DDoS (distributed denial of service) (25 % of respondents).

These results underscore the importance of defending against the two most prevalent threats—ransomware and phishing—and mitigating risks by implementing robust cybersecurity measures.

Additionally, the company's planned expenditure on cybersecurity was outlined, with a total of €50,000 allocated for the upcoming year. The most significant portion (€13,000) will go towards firewalls and intrusion detection systems, followed by €10,500 for secure network design and €9,000 for employee training.

To gather information on anticipated investments in cybersecurity protection measures for the upcoming year, experts from the IT and finance departments disclosed the planned percentage of the budget allocated to each cybersecurity management strategy. Participants provided valuable insights into organisational objectives and defence tactics against cyberattacks, along with statistics outlining their planned allocation of resources across various cybersecurity projects (Figure 3).

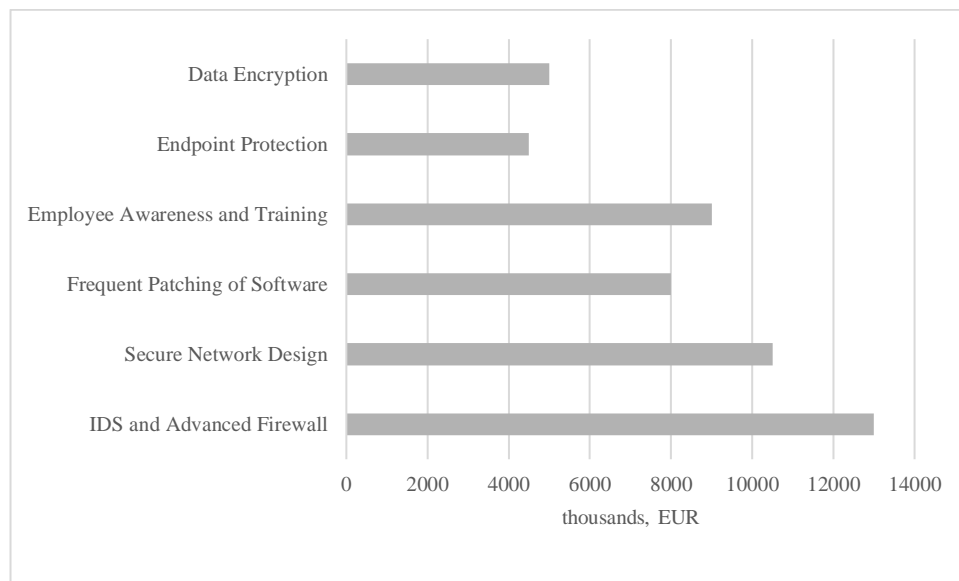


Figure 3: Projected cyberattack expenditure for the IT company (thousands EUR) (source: compiled by the authors)

The cybersecurity protection plans for the forthcoming year, as planned by the IT and finance departments, are outlined in the image (Figure 3). The budget allocation includes:

1. IDS and an advanced firewall (13,000 EUR).
2. Secure network design (10,500 EUR).
3. Frequent patching of software (8,000 EUR).
4. Employee awareness and training (9,000 EUR).
5. Endpoint protection (4,500 EUR).
6. Data encryption (5,000 EUR).

In summary, the findings indicate that substantial resources are dedicated to advanced firewall and intrusion detection systems, as well as employee education and awareness programs, which emphasise the importance of human factors in cybersecurity.

4.3. Ranking of cybersecurity measures

The Global Cost of Cyber Risk Calculator and survey data were utilised, together with the TOPSIS approach, to identify the best cyberattack management plan for the IT company named *S*. This strategy

aids the business in evaluating various tactics and determining the best ways to improve cyber resilience and draw in clients.

Table 3: TOPSIS analysis results: cybersecurity investment prioritisation for the IT company (source: compiled by authors)

Cybersecurity Measure	Proximity to Ideal Solution
Advanced Firewall and IDS	≈ 0.912
Secure Network Architecture	≈ 0.811
Employee Training and Awareness	≈ 0.799
Regular Software Patching	≈ 0.660
Data Encryption	≈ 0.576
Endpoint Protection	≈ 0.523

The TOPSIS analysis for the IT company evaluated cybersecurity strategies based on effectiveness scores, with a score of 0.912, indicating that advanced firewall and intrusion detection system implementation comes in first place. This tactic is essential for strengthening cybersecurity defences since it efficiently monitors and filters network traffic.

The necessity of creating a resilient and secure network infrastructure is highlighted by the tight second-place score of 0.811 for secure network architecture. In order to keep data integrity and prevent unwanted access, a well-designed network topology is necessary. Third-placed employee training and awareness (0.799) emphasises the importance of teaching staff members about cyber hazards and best practices. In order to recognise and reduce potential risks, having an informed staff is essential.

Regular software patching, with a score of 0.660, is still important for quickly addressing vulnerabilities, but it has a less immediate effect than solutions with higher rankings. By encoding data, data encryption (with a score of 0.576) helps to secure sensitive information; however, its efficacy is not as high as that of other tactics. With a score of 0.523, endpoint protection—which focuses on protecting specific devices, such as PCs and mobile phones—has the lowest rating. Although significant, its overall efficacy is lower than that of more expansive network and people-focused tactics.

In conclusion, the IT company's cybersecurity defences will be greatly strengthened by giving top priority to the installation of modern firewalls and intrusion detection systems, secure network architecture, and thorough staff training. When all of these safeguards are taken together, the organisation's data and activities are adequately protected against cyber threats.

5. Discussion

The findings of this study highlight that cybersecurity in the digital era has evolved into a multidimensional managerial challenge rather than a purely technical issue. This aligns with the findings of other studies (e.g., Mahmoudi, 2025; Fauzi et al., 2023; Fotis, 2024), which state that cybersecurity has emerged as a significant

managerial challenge in the digital era due to the increasing reliance on digital technologies and the growing sophistication of cyber threats. Proactive management of cyber risks is essential for effective cybersecurity and risk mitigation, especially in the IT industry. To defend against threats such as malware, phishing, ransomware, and insider attacks, IT companies must implement comprehensive strategies that integrate advanced technology, human factors, and organisational policies. Ensuring operational resilience and the ability to adapt to the evolving cyber threat landscape requires interdisciplinary collaboration and ongoing improvement in cybersecurity measures.

The study demonstrates how data-driven risk assessment tools can be used to evaluate and manage cybersecurity costs in IT companies operating in the digital era. Scientists agree (e.g., Jeyavim & Parkavi, 2025; Randive et al., 2023; Ouhssini et al., 2024) that the shift from technical protection to data-driven decision-making represents a transformative change in how organisations operate. By leveraging advanced technologies and fostering a data-driven culture, organisations can enhance their decision-making processes, gain a competitive edge, and navigate the complexities of the modern digital landscape. However, this transition requires addressing significant challenges related to data management, privacy, and organisational change to fully realise the potential of data-driven insights.

Many studies (e.g., Colabianchi, 2025; Ghelani, 2022; Randive et al., 2024; Sharma, 2023) indicate that human factors and organisational change are integral to effective cybersecurity management. By prioritising human factors engineering, fostering a cybersecurity culture, leveraging HR functions, and implementing strategic communication and training, organisations can significantly enhance their cybersecurity posture. Strong leadership and integrated frameworks further support these efforts, ensuring a holistic approach to managing cybersecurity risks.

In conclusion, by strategically directing resources toward these key cybersecurity measures, the IT company can enhance its resilience against rising cyber threats and ensure the uninterrupted and secure operation of its business activities, while optimising its financial performance in risk management. The projected growth in cyber-attack damages further emphasises the need for continuous investment in cybersecurity strategies to mitigate risks effectively.

Overall, the discussion demonstrates that cybersecurity in the digital era is a complex managerial challenge shaped by technological, organisational, and human factors. The findings contribute to a broader understanding of how managers can enhance cybersecurity resilience by integrating strategic planning, cultural development, and regulatory awareness into their decision-making processes.

6. Conclusions

This study examined how data-driven risk assessment tools can be used to evaluate and manage cybersecurity costs in IT companies operating in the digital era. By combining sector-level cyber risk forecasting with firm-level proportional analysis and multi-criteria decision-making, the research provides a structured approach to understanding the financial implications of cyber threats and prioritising defensive investments.

The findings reveal a significant projected increase in cyber-attack costs for both the Lithuanian IT sector and the analysed IT company, underscoring the growing managerial importance of cybersecurity in digital business environments. The TOPSIS-based evaluation further shows that technological measures, such as advanced firewalls and intrusion detection systems, together with organisational measures like secure network design and employee training, play a decisive role in mitigating cyber risks.

From a management perspective, this study highlights a shift from reactive cybersecurity spending toward proactive, data-driven decision-making. Rather than treating cybersecurity as a purely technical issue, IT managers are encouraged to integrate cyber risk cost forecasting into strategic planning and resource

allocation processes. In this sense, cybersecurity management becomes an integral part of organisational adaptation to the digital era.

This study has limitations. It focuses on a single industry and one representative company, and relies on forecast-based estimates rather than realised loss data. Future research could extend the framework to other sectors, incorporate dynamic threat modelling, or examine how cybersecurity investment decisions evolve over time. Nevertheless, the study offers valuable insights into how digital risk analytics can reshape managerial practices in the context of ongoing digital transformation.

References

- Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2019). A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities. *IEEE Communications Surveys and Tutorials*, 21(2), 1851–1877. <https://doi.org/10.1109/COMST.2019.2891891>
- Colabianchi S., Costantino F., Nonino F., Palombi G. (2025). Transforming threats into opportunities: The role of human factors in enhancing cybersecurity. *Journal of Innovation and Knowledge*, 10 (3). DOI: 10.1016/j.jik.2025.100695
- Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *Geneva Papers on Risk and Insurance: Issues and Practice*, 47(3), 698–736. <https://doi.org/10.1057/s41288-022-00266-6>
- Dreyer, P., Jones, T., Klima, K., Oberholtzer, J., Strong, A., Welburn, J. W., & Winkelman, Z. (2018). *Estimating the Global Cost of Cyber Risk: Methodology and Examples*. chrome-extension://efaidnbmnnnibpcajpcgiclfefindmkaj/https://www.rand.org/content/dam/rand/pubs/research_reports/RR2200/RR2299/RAND_RR2299.pdf
- Fauzi, R., Mahmud, I., & Hassan, H. (2023). Proactive approaches in mitigating cyber risk: A review of organisational resilience frameworks. *Journal of Information and Organizational Security*, 12(3), 76-90. <https://doi.org/10.1002/9781119843315.ch5>
- Fotis, F. (2024). Economic Impact of Cyber Attacks and Effective Cyber Risk Management Strategies: A light literature review and case study analysis. *Procedia Computer Science*, Vol. 251, 471-478. <https://doi.org/10.1016/j.procs.2024.11.135>.
- Ghelani, D., Hua, T., Koduru, S. K. R. (2022). Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking. 10.22541/au.166385206.63311335/v1.
- Howell T., Rojas-Segura J., Martinez-Villavicencio J., Rodriguez Bravo C. (2025). Cybersecurity Vulnerabilities in Companies: A Case Study [Vulnerabilidades en la Seguridad Cibernética de Empresas: Un Estudio de Casos]. Proceedings of the LACCEI international Multi-conference for Engineering, Education and Technology. DOI: <https://dx.doi.org/10.18687/LACCEI2025.1.1.1773>
- Ilany-Tzur, N., Fink, L. (2025). Device and risk-avoidance behavior in the context of cybersecurity phishing attacks. *International Journal of Information Management*, Vol. 84. <https://doi.org/10.1016/j.ijinfomgt.2025.102919>.
- Inayat, U., Farzan, M., Mahmood, S., Zia, M. F., Hussain, S., Pallonetto, F. (2024). Insider threat mitigation: Systematic literature review. *Ain Shams Engineering Journal*, 15(12). <https://doi.org/10.1016/j.asej.2024.103068>.
- Cremer, F., Sheehan B., Fortmann M., Kia A. N., Mullins M., Murphy F., Materne S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *Geneva Pap Risk Insur Issues Pract*. 47(3):698-736. doi: 10.1057/s41288-022-00266-6.

Jacobs, T., Junge, T., & Pastewka, L. (2017). Surface Topography: Metrology and Properties. Quantitative characterisation of surface topography using spectral analysis. In *Surf. Topogr.: Metrol. Prop* (Vol. 5). DOI 10.1088/2051-672X/aa51f8

Jeyavim S. R. C. & Parkavi K. (2025). Software-defined Networking Controller for Detection of DDoS Attacks Based on Deep Neural Networks. *International Journal of Modern Education and Computer Science*, 17 (4), pp. 1 – 18. DOI: <https://doi.org/10.5815/ijcnis.2025.04.01>

Ji J., Mogos G. (2025). Malware Traffic Analysis using Machine Learning. *ACM International Conference Proceeding Series*, pp. 62 – 67. DOI: 10.1145/3718391.3718417

Eisenbach, T., Kovner, M. Lee, A., Junho, M. (2021). Cyber risk and the U.S. financial system: A pre-mortem analysis Standard-Nutzungsbedingungen. <http://hdl.handle.net/10419/241102>

Liu, X., Ahmad, S. F., Anser, M. K., Ke, J., Irshad, M., Ul-Haq, J., & Abbas, S. (2022). Cyber security threats: A never-ending challenge for e-commerce. *Frontiers in Psychology*, 13. <https://doi.org/10.3389/fpsyg.2022.927398>

Malavasi, M., Peters, G. W., Trück, S., Shevchenko, P. V., Jang, J., Sofronov, G. (2026). Cyber risk taxonomies: statistical analysis of cybersecurity risk classifications, *Insurance: Mathematics and Economics*, 126, 1-16. <https://doi.org/10.1016/j.insmatheco.2025.103167>.

Mahmoudi A. (2025). Cybersecurity Challenges in Smart Economies: Managing Risks in a Digital-First World. *Dynamic and Safe Economy in the Age of Smart Technologies*, pp. 139 - 154. DOI: 10.4018/979-8-3693-4369-2.ch009

Qasaimeh, G. M., & Jaradeh, H. E. (2022). The Impact of Artificial Intelligence on the Effective Applying of Cyber Governance in Jordanian Commercial Banks. *International Journal of Technology, Innovation and Management (IJTIM)*, 2, 68-86. <https://doi.org/10.54489/ijtim.v2i1.61>

Odeyar S. V., Thejaswini K. M., Lolakshi P. K., Chaithra K. N. (2025). Reactive versus Proactive Cyber Security and Real Time Threat Protection. *Cyber Security in Business Analytics*, pp. 66 - 81. <https://doi.org/10.1201/9781003540045>

Ouhssini, M., Afdel, K., Akouhar, M., Agherrabi, E., Abarda, A. (2024). Advancements in detecting, preventing, and mitigating DDoS attacks in cloud environments: A comprehensive systematic review of state-of-the-art approaches. *Egyptian Informatics Journal*, Vol. 24. <https://doi.org/10.1016/j.eij.2024.100517>

Randive, K., Mohan, R., Sivakrishna, A. M. (2023). An efficient pattern-based approach for insider threat classification using the image-based feature representation. *Journal of Information Security and Applications*, Vol. 73. <https://doi.org/10.1016/j.jisa.2023.103434>.

Sharma, A. (2024). The impact of cybersecurity breaches on big businesses. *International Journal of Advanced Research*. 12. 10-25. 10.21474/IJAR01/19614.

Shih H.-S. (2022). TOPSIS Basics. *Studies in Systems, Decision and Control*, 447, pp. 17 - 31. DOI: 10.1007/978-3-031-09577-1_2

Solfa, F. D. G. (2022). Impacts of Cyber Security and Supply Chain Risk on Digital Operations: Evidence from the Pharmaceutical Industry. *International Journal of Technology, Innovation and Management (IJTIM)*, 2(2). <https://doi.org/10.54489/ijtim.v2i2.98>

Yarovenko, H. (2020). Evaluating the threat to national information security. *Problems and Perspectives in Management*, 18(3), 195-210. doi:10.21511/ppm.18(3).2020.17