risks

MDPI

Article

Dynamic Assessment of Cyber Threats in the Field of Insurance

Lukáš Pavlík *, Martin Ficek and Jakub Rak

Department of Civil Protection, Tomas Bata University in Zlin, Studentské nám. 1532, Mařatice, 686 01 Uherské Hradiště, Czech Republic
* Correspondence: lpavlik@utb.cz

Abstract: The area of digital technologies is currently the subject of many cyber threats, the frequency of which is increasing. One of the areas of cyber security is also the creation of models and estimates of the process of cyber threats and their possible financial impacts. However, some studies show that cyber-threat assessment to identify potential financial impacts for organizations is a very challenging process. A relatively large problem here is the detection of scenarios of cyber threats and their expression in time. This paper focuses on the design of an algorithm that can be applied to the field of cyber-threat assessment in order to express the financial impacts. The study is based on an in-depth analysis of the insurance industry. The results obtained in our research show the importance of the time perspective for determining the potential financial impacts of cyber threats for the field of insurance.

Keywords: cyber threat; risk; insurance; impact; financial damage; information system

JEL Classification: C590; G170

Citation: Pavlík, Lukáš, Martin Ficek, and Jakub Rak. 2022. Dynamic Assessment of Cyber Threats in the Field of Insurance. *Risks* 10: 222. https://doi.org/10.3390/risks10120222

Academic Editors: Weidong Tian and Paolo Giudici

Received: 26 August 2022
Accepted: 14 November 2022
Published: 22 November 2022

1. Introduction

The protection of information systems and their components is of interest to many managers and executives in organizations. As the sophistication and frequency of cyber-attacks grows, the insurance sector has also begun to respond to this area. The first cyber-security products began to appear in the early 21st century (Siegel et al. 2002). At this time, the first insurance offers began to appear on the insurance market, which was focused on solving and minimizing the financial impacts of cyber threats (Majuca et al. 2006). In terms of development, the first insurance products of this type began to appear in the USA, Germany and the United Kingdom. At present, the offer of this insurance is the widest in these parts of the world (Bradford 2015; Biener et al. 2015).

The economic impact of cyber-attacks can be very extensive. Information systems are not only made up of hardware and software, but also the human factor, which is also the biggest vulnerability in an organization's information environment. The financial impacts of the realized cyber-threat can affect the entire structure of the organization and spread further with the help of the so-called domino effect. For this reason, cyber security is taking on a different dimension. It is therefore no longer just a technical problem, but also an economic, legal and security problem. If we focus on the issue of cyber-threat insurance from the point of view of legislation, then it is mainly the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons in connection with the processing of personal data and on the free movement of such data and on the repeal of Directive 95/46/EC (General Data Protection Regulation), or the Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to ensure a high common level of security networks and information systems in the Union (Bahşi et al. 2019). The economic impact of cyber threats is influenced by three basic factors (Martinelli et al. 2017; Hofmann 2007).

These are mainly:

(1) Time (duration of the cyber-attack);
(2) Scope (extent of impact on the organization's information environment);
(3) Degree of interaction (degree of severity of the cyber threat in combination with the impact on the affected area in the organization).

Assessing the potential financial impact of cyber threats on an organization's information environment is of interest to some research organizations and insurance companies around the world. Although there are many tools for risk analysis, the question of assessing the financial impact of these risks merits further attention. In the scientific literature, we can find the work of several authors who deal with this issue (Palsson et al. 2020; Romanosky 2016). Nevertheless, the area of determining the financial impact of cyber threats on an organization's information environment is still a subject of research in the insurance industry. Insurance companies often use a questionnaire survey to determine the insurance premium in combination with the risk analysis of a given information environment (Woods and Simpson 2017). However, this approach does not provide a comprehensive analysis of all potential cyber threats and their potential financial implications. The areas that may be most affected by the impact of cyber threats are usually not taken into account here, and therefore it is rather a qualified estimate. These areas represent the parts of the organization and its information environment that can be affected by cyber threats and in which the organization can incur financial losses. This fact is also caused by several factors (European Insurance and Occupational Pensions Authority 2019).

Compared with other types of insurance, standard actuarial procedures cannot be applied to insurance against cyber threats. The main reason is mainly the nature of cyber-attacks and their possible course. Whereas with other types of insurance (such as natural threats, etc.) it is possible to model various future situations of property damage, or health effects of the threat, this model is very difficult for cyber-attacks. This is mainly due to the rapid development of the types of these threats and the high variability of their possible course. In most cases, the modeling of future claims for other types of insurance is based on the analysis of historical data, on the basis of which the possible future development and impact of adverse events is modeled (Franke 2017). This approach cannot be applied to cyber threats. The individual types of cyber threats and their course are changing very rapidly, and therefore it is not possible to predict, based on historical data over the past few years, what the situation will be next year or how much impact cyber threats can cause.

The second important factor that complicates the estimation of future damage is that cyber threats take place in a virtual environment that is not defined by any physical laws on the basis of which their development could be predicted (Woods et al. 2017). In the case of other types of adverse events that take place in our ordinary reality (for example, natural threats), it is possible to estimate the possible course of a given phenomenon and its effects, at least on the basis of certain physical indicators. For cyber threats, the application of such a procedure is almost impossible. For current insurance institutions, the issue of determining possible future damage caused by cyber threats is still a major challenge (Bandyopadhyay et al. 2009). There is a relatively large number of risk-analysis tools. However, their application still does not bring results that would be widely usable for this type of insurance (HM Government & Marsh Ltd. 2015; Krautsevich et al. 2011).

This paper is divided into several parts. The chapter entitled Theory Background describes the essence of cyber threats and their impacts on the organization's information environment. The proposed algorithm is defined in the Methods chapter, and its development is also described. The results of the questionnaire survey, which were used as a basis for the proposed algorithm, are also described here. The endangered elements of the organization and their assessment are characterized here, and represent the areas that can be most affected by the impact of cyber threats. In the case study, which is divided into two subsections, the proposed algorithm is applied to a selected organization. There is also a risk analysis, with an emphasis on expressing the potential financial impacts of the most serious cyber threats on the organization's information environment. In the Discussion and

Conclusion of this paper, an evaluation of the achieved results and a proposal for possible future development are performed.

2. Theory Background

Based on the nature and variability of cyber threats, determining financial impacts is very difficult. The insurance coverage does not then fulfill the given purpose, i.e., compensation for financial damages, and the agreed insurance does not bring the required benefit for the organization (Marsh Insights 2015). Compensation for the financial impact of cyber threats on the organization's information environment in the form of insurance is of interest to many types of organizations. Nevertheless, it cannot be said that this type of insurance is for every organization. The subjects of insurance are most often small and medium-sized organizations that focus on production, trade or services. This is usually a relatively well-designed and stabilized information environment that is not very risky (Marotta et al. 2017; Kaspersky Lab ICS CERT 2018; Young et al. 2016). However, insurance with a focus on compensation for corporate damage caused by cyber threats is not suitable for larger organizations and operations such as airports. This type of organizational structure is very complex, and there are a large number of processes and information-flows in real time that could be analyzed under current methods and approaches to this problem (Farnan and Nurse 2016).

In addition to the renewal of hardware and software, data are also the subject of insurance, which is aimed at compensating for financial damage caused by cyber threats (Schwartz 2019). In organizations, data are the most valuable asset, and modification or loss can be a major burden on organizations (Palsson et al. 2020). Hardware or software equipment is relatively simple to recover, but intangible assets that represent data and information are very difficult to reconstruct (Meland and Seehusen 2018; Lin et al. 2022). In this case, we can talk about another challenge in this area. Financial valuation of data and information that the organization works with within its information environment is very difficult, due to the application of current asset-valuation methods. In essence, there is no comprehensive algorithm to value this asset as accurately as possible.

Other areas that can be significantly affected by the impacts of cyber threats include the organization's reputation. Every organization builds its reputation or brand for many years, and it is a long-term process that depends on many factors. This can be a period of time (i.e., the time for forming a good name or brand). Other factors include the financial resources we invest in this process or the human factor involved in co-creating a reputation (Eling and Wirfs 2016). All these elements are an integral part of the process of building an organization's reputation, and insurance should focus on cyber threats and their impacts on this area. The organization's reputation, along with data and information, is also one of the most valuable assets (Millaire et al. 2018). It is possible that violation may result in liquidation for the organization. However, it is important to emphasize here that not every cyber incident can have a significant impact on the reputation of an organization (Shetty et al. 2010).

Based on a study of the available literature and case studies, it can be stated that a comprehensive methodological approach or algorithm for determining the potential impacts of cyber threats is not known. For comparison, we can also mention the cyber value-at-risk system, which is used to express the potential financial loss caused by the impact of cyber threats (Erola et al. 2022). The application of this system can provide an analysis of possible financial impacts; however, this statement applies on a fairly general level. If we use this system, we can estimate possible future financial losses that are caused by the impact of a cyber threat, but we will not receive a specific financial amount. In the professional literature, we can also find other approaches to express the potential impacts of cyber threats, which are based on factors such as gross losses and the frequency of cyber threats (Aldasoro et al. 2020). Even if this approach does not include other indicators in determining the financial impacts of cyber threats, we can obtain other interesting information with this method. There is, for example, the relationship between the future

development of cyber threats and stronger supervision. There are also purely mathematical approaches to this problem, which are based on Shapley-Lorenz values (Giudici and Raffinetti 2022). This approach involves the comparison of several variables, such as the type of victim, the type of attacker, the attack technique, and the continent where the cyber incident occurred. Applying this approach can provide us with a prediction of the severity of cyber incidents. However, this approach does not include a financial expression of potential damages that may be caused by cyber threats. The current approach of insurance institutions to this problem is mostly based on a combination of several existing risk-analysis methods. In many cases it can be a FAIR (Factor Analysis of Information Risk) method (Böhme 2010). This method of risk analysis in the field of digital technologies is based on a taxonomy of factors that interact and thus have a specific relationship to risk. The main objective of this method is to determine the probabilities for a specific risk event and potential losses. The FAIR method is based on IT-security-management standards, such as a number of ISO/IEC 27000 standards. Although the FAIR methodology provides a relatively comprehensive approach to assessing cyber-threat risks and their potential impacts, there are areas that remain uncovered. There is, for example, a time view of the development of cyber threats. Every cyber threat evolves over time.

The development of these threats over time can be divided into two aspects:

(1) The development of the cyber threat from the perspective of sophistication;
(2) The development of the cyber threat from the point of view of the implementation of its course.

3. Methods

The algorithm, which is the result of the research work of the authors of this paper, has been developed from 2015 to the present. In the years 2015 to 2019, it was developed as part of a doctoral thesis. In this time period, the basic phases of the whole algorithm were defined, including verification options. Since 2019, the algorithm has been further developed and expanded, with new knowledge. These scientific findings are based on the current state of the field of cyber-threat insurance.

3.1. Development of Algorithm

One of the main sources for the design of the algorithm for determining the impact of cyber threats was a questionnaire survey. The resulting conclusions were formulated primarily on the basis of consultations in selected organizations located in the Czech Republic and Germany. These consultations took place in the form of a questionnaire survey, too. Based on the results of the questionnaire survey, the basic requirements and objectives for the proposed algorithm were formulated. It was mainly a matter of defining endangered elements (areas) of the information environment of organizations that may be most affected by the financial impact of cyber threats.

A part of the questionnaire survey was also to find information on the requirements of organizations from insurance companies. The research focused on possible financial compensations by insurance providers against cyber threats to insured organizations. Selected sectors in which the organization operates are shown in the following chart (Figure 1). The questionnaire survey was conducted in 20 organizations. Due to their size and number of employees, these organizations can be classified as small or medium-sized enterprises. These were exclusively organizations from the private sector, which differ in their essence of business and information environment. Because the questionnaire is focused on the field of cyber security, some organizations were not willing to cooperate, mainly because of the sharing of sensitive data about their information systems.

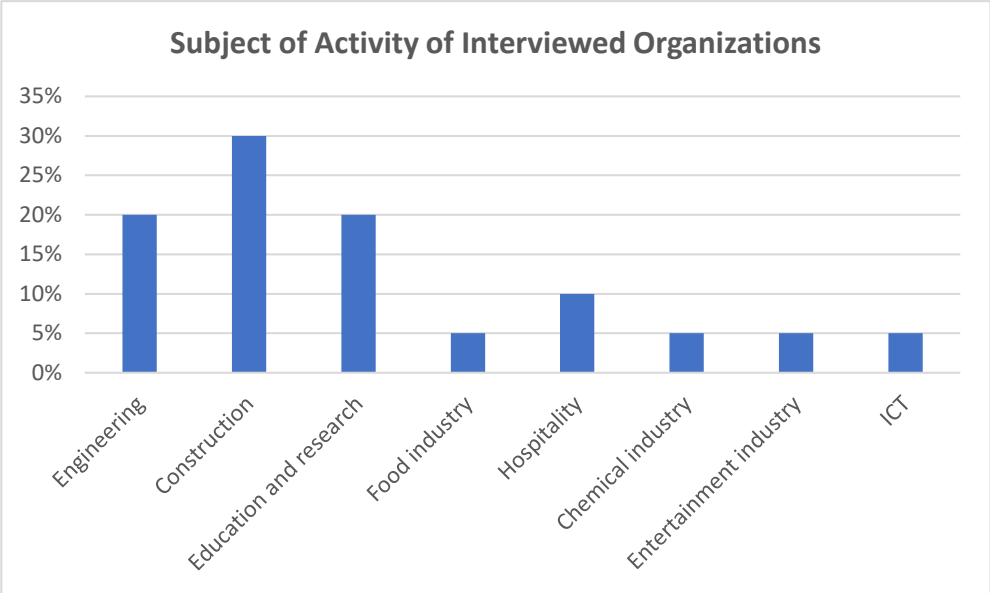

Figure 1. Subject of activity of interviewed organizations (own resource).

A questionnaire is a widely used method for addressing selected target groups, in this case reference groups. A total of 26 questions are constructed in the questionnaire. These questions are divided into six categories, according to their professional focus.

These are the categories:

(1) Information about the organization that is the subject of the questionnaire survey;
(2) The organization's information system;
(3) Data security and restorability of the organization's function;
(4) Types of cyber threats;
(5) Readiness of the organization in the field of cyber security;
(6) The expected extent of coverage against cyber threats.

The questionnaire was developed based on the study of the professional literature. The areas covered mainly related to the issue of insuring organizations against cyber threats. Each category is focused on a different part of this issue, with the aim of obtaining a comprehensive overview of the perception of this type of insurance among small and medium-sized enterprises in the Czech Republic. The questions are designed to determine which areas of the information environment may be most affected by the impact of cyber threats, and whether insurance against these threats is an appropriate solution for organizations. During the implementation of the questionnaire survey, senior employees of the approached reference-objects were informed that it was a research study and that the names of the interviewed organizations and individual employees would not be published. The questionnaire was presented to the senior employees with a verbal supplement. If any of the employees expressed misunderstanding of any of the questions presented, this question was explained to him verbally. The average duration of the interview and filling out of the research questions was 50 min. A percentage expression was used in the evaluation of the conducted research. The results of the questionnaire survey are divided into six separate categories, according to the focus of the questions.

For a more precise characterization of the interviewed subjects, their basic attributes are described here, and include:

Scope of business:

(1) Number of employees;
(2) Annual turnover;
(3) Number of units.

The names of the interviewed organizations are not listed here, for reasons of anonymity and reputation.

Other organizations that have also been consulted and which conducted discussions focusing on cyber threat insurance include insurance companies and universities. However, this type of organization was not included in the questionnaire survey, and information was collected on the basis of individual meetings.

The proposed algorithm unifies the various views and areas that are necessary to express the insurance value in the field of cyber-threat insurance. These are mainly economic and IT-security aspects of risk and its potential impacts. In the case of applying the proposed algorithm, the insurance value is defined as the highest financial loss that can occur on tangible or intangible property as a result of a cyber incident (Czech Association of Insurance Companies 2022). This financial indicator in the form of the insurance value can be used by the insurance company primarily as a basis for determining the optimal insurance-coverage for the given organization.

The proposed algorithm unifies the various views and areas that are necessary to express the insurance value in the field of cyber-threat insurance. These are mainly economic and IT-security aspects of risk and its potential impacts. Based on the needs of the proposed algorithm, it was necessary to include the interaction between the cyber threats and its impacts on endangered elements of the information environment. The interaction of these two factors is relatively important in determining the possible financial impacts of cyber threats.

The designed mathematical formula has been extended by an element of time, which to our knowledge is an important factor in determining the possible financial damages that can be caused by cyber threats. The course of a specific cyber-threat and its duration significantly determines its impact on the information environment of the organization. The type of cyber threat is also essential in the process of determining the timeline. Some cyber threats can only be aimed at, for example, damaging or destroying the physical equipment of an organization's information system. For this type of threat, which can be ransomware, its duration is relatively short. In contrast, a cyber threat such as a hacker attack on an organization's production system can be much longer. The so-called domino effect can occur with this type of threat. The effects of such a cyber threat may affect other parts of the organization that appear to be unrelated to the information environment. These are, for example, the name reputation of the organization, relations with suppliers, subscribers and customers, or fines for non-compliance with obligations to third parties. In Figure 2 we can see the scheme of the algorithm for dynamic risk-assessment.

3.2. Defining a Framework of Risk Assessment

To express the degree of risk in relation to cyber threats and their effects on the information system, it is necessary to establish a mathematical formula. This mathematical formula was designed based on the basic relationship between the level of risk, potential impacts on endangered elements, and time frame. The following mathematical formula was proposed, to determine the risk level of selected cyber threats:

$$R = P * E * V * T \quad (1)$$

where:

R = degree of risk;
P = probability of threat;
E = value of endangered element (impact);
V = vulnerability of endangered element to cyber threats;
T = time frame of cyber threat (degree).

The probability of a threat is expressed on a scale of one to five. Each of these five degrees of probability is assigned a decimal range that expresses the degree of risk. Number one is the least likely threat and number five indicates the most likely threat to the

organization's information environment. Cyber threats are evaluated in the next step by individual probability levels.

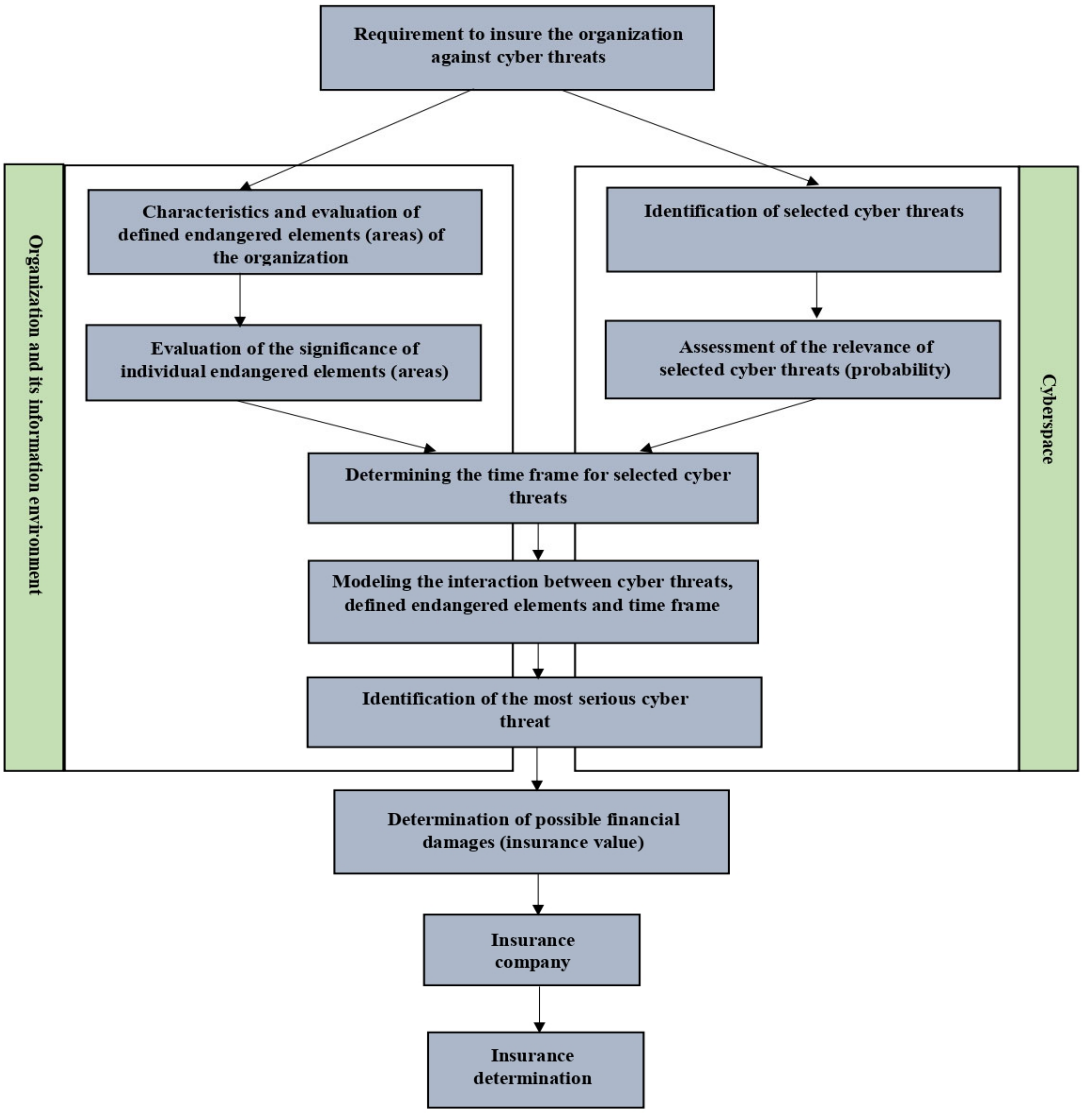

Figure 2. Scheme of algorithm for dynamic risk assessment (own resource).

The individual levels of probability are assigned a decimal range, as we can see in the following table (Table 1). The number of degrees of probability was determined on the basis of the usual distribution for risk analysis, which is defined in the ISO standard 27005. The distribution of the decimal expression for individual degrees of probability was determined on the basis of the results of research that was carried out for the dissertation of one of the authors of this paper, and which was presented in a previous part of the research (Pavlík 2019).

Table 1. Decimal scale of probability of threat (own resource).

Probability of Threat	Decimal Expression
1	0–0.25
2	0.26–0.45
3	0.46–0.65
4	0.66–0.85
5	0.86–1

The value of endangered elements (areas) is also divided into five degrees. Number one is the least important element for an organization in terms of securing its information system. The most important element for an organization is marked with number five. Each of these vulnerable elements represents an area that may be most affected by the impact of cyber threats and in which the organization may suffer significant financial damages. These endangered elements represent areas of the information environment that can be significantly affected by the impact of cyber threats. Disruption or destruction of these elements can also be a major financial burden for organizations.

The vulnerability of endangered elements to cyber threats reflects the interaction of these two levels, which have a significant impact on the expression of future financial implications for the organization. Each endangered element has a different vulnerability to cyber threats. For some endangered elements, the interaction with the selected cyber threat does not take place. In these cases, there are no potential financial implications. The possible interaction is expressed in the risk matrix, in which we can then see all the relationships of the above-mentioned members of the proposed mathematical formula. From the vulnerability matrix, it is possible to identify cyber threats that have the greatest possible financial impact in correlation with the degree of threat of the selected endangered elements. Within the determination of the most serious possible scenarios, four cyber threats are always selected, for which the highest level of risk is expressed. These threats are compared using Saaty's method. Using the weights assigned to the individual criteria and the geometric mean, we can determine the most considered cyber threat in terms of potential financial impacts. The expression of the interaction between cyber threats and vulnerabilities is given in the "Results" section. This risk chart is the first result of the application of the proposed algorithm for dynamic risk-assessment, which expresses the potential financial impacts on the selected organization.

Defining a Pricing of Endangered Elements

The following endangered elements are used to identify potential impacts on an organization's information environment. For each endangered element, a method of its financial expression is proposed.

(1) Hardware

The area of hardware includes not only computer devices and their accessories, but also other technical components that ensure the functions of the information system. We can apply this valuation option if the hardware has a lower price than EUR 1622.

Valuation at acquisition costs is the method is applied in the case of assets that are acquired for consideration (the price includes related costs such as installation and transportation, patents and licenses or exploration, geological and other works). Costs related to the purchase price may also include interest on the loan.

Repurchase valuation costs represents the price for which the asset was acquired at the time of its entry into accounting, i.e., a deposit of tangible assets, tangible assets as a gift or tangible assets acquired free of charge on the basis of financial leasing (in cases where the actual costs of creating the asset cannot be ascertained).

Actual costs are tangible assets that have been created by the business itself. These are direct or indirect costs that were incurred in the course of production or other activities (Pavlík 2019).

Another way of valuing hardware is based on its current residual value, which arises when depreciating long-term tangible assets that have a higher price than EUR 1622. As part of the expression of this type of property, the accelerated depreciation method was chosen according to the following formula:

In the first year:

$$O_n = \frac{PC}{K} \quad (2)$$

In the following year:

$$O_n = \frac{(2 * ZC)}{(k - n)} \quad (3)$$

where:

On = depreciation;
Pc = purchase price;
ZC = net book value;
K = coefficient in the first year[1];
k = coefficient valid in the coming years[2];
n = year of depreciation.

(2) Lost turnover

The following formula is designed to express lost turnover

$$U_Z = \sum_{i=1}^{n} CV_h * \sum_{i=1}^{n} H_v \quad (4)$$

where:

U_z = last year's turnover;
CV_h = the price of a normal number of products made in one hour;
H_v = the number of hours when the products are not produced.

(3) Fees

Fees related to the realization of a cyber threat can be applied in several cases. If this is the type of organization in which the main business is the production process, then this organization may be sanctioned for non-compliance with the production plan. This situation can occur in the event of a disruption in the function of the organization's information system, whose main task is to ensure the operation of production machines. If the required number of products were not fulfilled within the time schedule, the organization would also incur large financial losses.

These fines can be issued either by the central management of the organization (in the event of a malfunction of the information system at the branch of the organization), or the fine can be issued by the supplier of the material or service. If the material is not sold by the supplier within a certain time interval, these third-party entities may experience a loss of profit. A similar situation can also occur on the customer's side. If the receiving entity does not receive the relevant product or service from the organization within a certain period of time, it loses the profit from the sale. This situation also occurs with an organization that has become the subject of a cyber incident. Another entity that can impose sanctions on a given organization is the competent supervisory authority. This policy is governed by the General Data Protection Regulation (GDPR).

No predefined formula can be used to represent this category financially. The amount of the fine is always an individual matter, and depends on supplier–customer relationships. In the case of the general GDPR regulation, the amount of fines is set between EUR 10,000,000 and EUR 20,000,000, or 4% of the company's total turnover (Pavlík 2019).

(4) Software

For the purposes of this research, the amount of cost that would have to be incurred to reinstall the software in the event of a breach will be used. Since the organization owns a license to operate the software tools, it is not necessary to repurchase the software at a new price. There may also be a situation where the software is acquired and tied to the hardware it was purchased with; however, this possibility is not very likely in the case of small and medium-sized enterprises (Pavlík 2019).

(5) Data reconstruction and recovery costs

The cost of data reconstruction and recovery can be defined as the costs incurred for the recovery of data resources, which can be represented by hardware and software

resources. In the event of a breach of these data resources, stored or backed-up data may be irretrievably lost or damaged. It is also possible to determine the average cost of lost or stolen data from available statistical sources. This average cost is reported to be USD 141 per person (Ponemon Institute 2017).

The following formula can be used:

$$N_R = C_D * \sum_{i=1}^{n} P_D \quad (5)$$

where:

N_R = data reconstruction costs;
C_D = the cost of lost or stolen data for one person;
P_D = the number of data items that can be lost or stolen.

(6) Damage to reputation

For the financial expression of reputation of the organization, it is necessary to characterize what is meant by this term. In the context of insurance against cyber threats, "damage to reputation" means future financial damage that will be caused by the realization of a cyber threat in certain areas of the organization. These areas are suppliers, customers and sponsors. These are financial resources that the organization may lose within a certain timeframe, due to an undesirable event. The reputation of the organization (also called goodwill in the field of economics), can be expressed financially using a mathematical apparatus. In this case, it is mainly about advertising and the image of the organization. In the area of advertising and image, the organization is evaluated as a whole, not only based on certain areas. To express the financial amount that reflects the area of advertising and image, it is necessary to measure the profitability of investments in this category. Furthermore, it is necessary to take into account the synergy that the company creates in order to reach the market.

In every organization, employees and managers invest their time, money and energy in creating the image of the organization. This process is primarily focused on approaching new customers, and suppliers, and maintaining existing contacts. For this reason, the calculations in this category are focused on this point (Pavlík 2019).

Staff qualifications

$$KBZ = \left(\frac{\sum_{i=1}^{n} X_i}{n} - \frac{\sum_{i=1}^{n} N_i}{n} \right) * 12 \quad (6)$$

where:

KBZ = qualifications of current employees;
X_i = monthly earnings from performances created by all current employees;
N_i = the monthly cost of training for all employees.

Advertising and Brand

$$RI = \left(PPK * \frac{\sum_{i=1}^{n} N_{ki}}{n} - PPK * \frac{\sum_{i=1}^{n} Z_{ki}}{n} \right) - \frac{\sum_{i=1}^{n} N_{ir}}{n} \quad (7)$$

where:

RI = advertising and image;
PPK = average income per client;
N_{ki} = new clients per year;
Z_{ki} = lost clients per year;
N_{ir} = advertising costs per year;
n = the value of the observed period.

Perspective

$$P = \frac{\sum_{x=1}^{n} X_i - X_{ip}}{n} \quad (8)$$

where:

P = perspective;
X_i = total income from the calculated year;
X_{ip} = total income from the previous year;
n = the value of the observed period.

(7) Costs of reporting data loss or leakage to supervisory authorities

In the case of insurance against cyber threats, the costs of reporting data loss or leakage to supervisory authorities should also be taken into account. In the case of loss or leakage of personal data, the time interval for reporting this event to the competent supervisory authority is 72 h, according to the general GDPR regulation. In this category, we may also include notifications to, and communications with, other parties affected by the data or information leak. This issue is also closely related to maintaining the reputation of the organization (Pavlík 2019).

For the purpose of expressing this parameter, the following formula may be used:

$$N_U = \sum_{i=1}^{n} (MZ_Z * H_M * T_U) \quad (9)$$

where:

N_U = the cost of loss or data-leakage notification;
MZ_Z = the number of customers or other entities that may be affected by loss or data leakage;
H_M = the hourly wage of employees who will be in contact with the entities concerned;
T_U = the number of hours spent on contacting the affected entities.

Another part of the proposed algorithm is the determination of the vulnerability of the endangered element to the cyber threat. This situation occurs in the event that during the realization of a cyber threat there is an impact on the endangered element (which may not always be the case). In this mathematical part, the relationship between the cyber threat and the endangered element is assessed. This relationship is also expressed on a five-point scale, where number 1 means the least impact of the cyber threat on the endangered element, and number 5 the highest impact of the cyber threat on the endangered element.

The last part of the process of determining the potential financial impacts of cyber threats on the organization's information environment is the time frame. The time dimension represents the expression of a cyber-threat scenario from the point of view of its development. The time frame is divided into five levels. Each of these levels represents the duration of the cyber threat in relation to its severity. To determine the degree of cyber threat in terms of time evolution, two dimensions of this problem are compared. The first dimension represents the time dimension, which is shown on the x-axis.

As we can see, the individual degrees of the time frame, which also determine the relevance of the cyber threat, are divided into five categories. Each of these degrees is characterized by a length of time that also affects the relevance of the cyber threat. The time length that is assigned to the individual degrees can be seen in the following table (Table 2). Each degree also contains a value that defines its importance in correlation with the relevance of the cyber threat. The time frame of individual levels was determined on the basis of an analysis of the principle of selected cyber threats. Expert studies that focus on this issue were also examined.

Table 2. Degrees of time frame (own resource).

Degree	Time Frame	Value of Relevance
1	Duration of a cyber threat up to 30 min	1
2	Duration of a cyber threat up to 3 h	2
3	Duration of a cyber threat up to 10 h	3
4	Duration of a cyber threat up to 24 h	4
5	Duration of a cyber threat more than 24 h	5

In the time dimension, it is hypothesized that the longer a cyber threat lasts, the more severe its impacts on the organization's information environment can be. The second dimension of this problem involves the relevance of the cyber threat, which is indicated on the y-axis. The severity of a cyber threat evolves over time. Therefore, if the duration of a cyber threat is shorter, then the effects of the implementation of this threat tend to be smaller. If the cyber threat lasts for a longer period of time, its potential impacts on the organization's information environment can be more serious. The time frame and individual degrees for the course of the cyber threat can be seen in Figure 3.

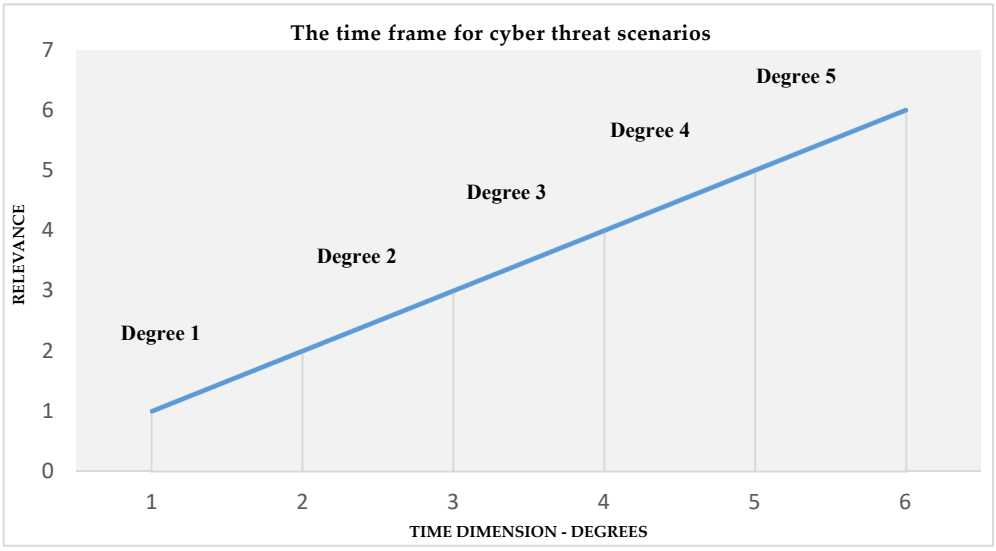

Figure 3. The time frame for cyber-threat scenarios (own resource).

It is necessary to mention that the time dimension is not relevant for every endangered element in the organization's information environment. If we take into account, for example, the interruption of the production process or business and thus also the generation of profit, the time dimension of the cyber threat represents a relatively big problem. In the event of an organization being unable to produce a profit, due to the realization of a cyber incident, this fact can have great a impact from a time point-of- view. The longer this state lasts, the greater the probability of more serous impacts of the cyber threat, thus also endangering the functioning of the given organization. In the event of a breach of data or information, or the possibility of fines by supervisory authorities, the time dimension does not represent a more serious problem. In this case, these are endangered elements that are more static from the point of view of the duration of the cyber incident, and their variability does not increase much with the duration of the cyber threat and its impacts.

4. Case Study Description

The verification of the algorithm on the reference object provides a statement about its applicability, functionality and possible benefits for the areas of insurance and cyber security. The algorithm was verified on a selected organization, which can be included in the category of small and medium-sized enterprises, and which operates in the Czech Republic.

The selected organization operates more than 400 retail stores throughout the Czech Republic. It was founded in the early nineties of the twentieth century, and has been operating up until the present. During this time, the company has secured a strong position in the domestic market, as evidenced by the company's annual turnover, which last year amounted to over EUR 280,000,000. The registered capital, which is divided among three partners, is more than EUR 3,000,000. The company specializes in food products (making up approximately 70% of the range), but also non-food goods (making up approximately 30% of the range).

The organization has approximately 2500 employees, who are located at various workplaces throughout the Czech Republic. All employees work with the Manas economic system, which is used for ordering goods, entering new goods into the catalog, communicating via e-mail with clients and with other company employees, performing cash closing, and designing and printing price tags and banners for goods.

4.1. Economic Part

Due to the scope of application of the algorithm on this example part of the organization, only the final results of the whole process are presented in the economic and IT-security part. This deals with the financial expression of endangered elements of the organization, in relation to the information system:

Hardware: EUR 313,811;
Lost turnover: EUR 843,339;
Fines: EUR 205,212;
Software: EUR 5808;
Data reconstruction and renewal costs: EUR 264,560;
Damage to good name: EUR 1,502,000;
Costs of reporting loss or data leakage: EUR 579,191;

The endangered elements of the organization are valued at a total amount of EUR 3,713,921.

4.2. IT Security Part

The first step is to identify the endangered elements in the organization, which are presented in Table 3.

Table 3. Values of endangered elements (own resource).

Endangered Elements	Identified Element	Value of Endangered Element
Hardware	Servers	4
	Computer systems	4
	Printers	2
	Production devices	3
Lost turnover	Lost turnover	5
Fees	Fees by supervisory authorities	3
	Fees from suppliers	4
Software	Database systems	4
	Special software (technological processes, production processes)	4
	Operating systems	4
Data reconstruction and recovery costs	Data reconstruction costs	5
	Data recovery costs	5
Damage to reputation	Damage to relationships with current customers	5
	Damage to relationships with potential future customers	5
	Damage to relationships with current suppliers and subscribers	5
	Damage to relationships with potential future suppliers and subscribers	5
Costs of reporting data loss or leakage to supervisory authorities	Help-desk costs	2
	Special investigative activity of a cyber incident	4
	Corrective measures	4

The second step is to identify cyber threats and the probability of their occurrence for the organization. The probability scale is again used for this step (see table above). A list of selected cyber threats is given in Table 4.

Table 4. Probability of cyber threats (own resource).

Cyber Threat	Probability of Threat	Example of Vulnerability
Ransomware	4	Insufficient antivirus protection of the information system, insufficiently educated employee
Intentional crime committed by a hacker	4	Insufficient antivirus protection of the information system, insufficiently educated employee
Unauthorized access	4	Insufficient security of the information system (irregular updating of passwords, easy access to the information system)
Malware	3	Insufficient antivirus protection of the information system, poor quality security software, insufficient e-mail security, insufficiently educated employee
Data leakage due to employee negligence	3	Failure to comply with security policies regarding the handling of internal and sensitive data of the organization
DDoS attack	3	Insufficient capacity and resilience of the computer network, insufficient network protection
Physical loss of data carrier (loss of laptop)	2	Insufficient security of the object in which the data carrier is located, risky behavior of the employee
Loss of data or disruption of the information system due to a lightning strike	1	Insufficient protection against lightning strikes (absence of lightning conductors, lightning arresters, etc.)
Failure of system	1	Insufficient technical maintenance of equipment, human-factor failure

The next step is to assign a degree from a time frame that expresses the possible duration of the cyber threat. Expression of this degree we can see in Table 5.

Table 5. Time frame degrees of cyber threat (own resource).

Cyber Threat	Degree	Time Frame
Ransomware	5	Duration of a cyber threat more than 24 h
Intentional crime committed by a hacker	4	Duration of a cyber threat up to 3 h
Unauthorized access	2	Duration of a cyber threat up to 3 h
Malware	5	Duration of a cyber threat more than 10 h
Data leakage due to employee negligence	5	Duration of a cyber threat more than 10 h
DDoS attack	4	Duration of a cyber threat up to 24 h
Physical loss of data carrier (loss of laptop)	5	Duration of a cyber threat more than 10 h
Loss of data or disruption of the information system due to a lightning strike	1	Duration of a cyber threat more than 24 h
Failure of system	3	Duration of a cyber threat up to 10 h

As we can see, ransomware has the most serious degree in terms of the impact of cyber threats over time. In the case of this cyber threat, the information system and its components may be encrypted and taken out of normal operation. An example can be the unavailability of logistics and production systems, which in the case of our organization focuses on the sale of food and non-food goods. The organization has several of its own production lines, and if they are shut down they will not be able to process material and produce products. The transport and delivery of goods and their storage could also be severely limited. Encrypting hard drives and other data sources is usually a matter that takes more than 24 h, which is why this cyber threat is assigned the highest value.

Decrypting data sources and gaining access to important information usually occurs only when addressing this security issue with experts in the field of digital technology and law.

Another cyber threat that is ranked highest in terms of impact on the organization and its information environment over time is malware. In the case of malicious-code acting in the organization's information environment, significant malfunctions or damage to hardware and software components may occur. The presence of malware goes unnoticed for a long time, and for this reason this cyber threat is dangerous from the perspective of the time dimension. Some malicious programs or software sometimes work in the information system for several months without anyone detecting their activity.

Data leakage due to employee negligence can be included among the other highest-rated cyber threats from the perspective of the time dimension. Although a data leak is a short matter from the point of view of the course of this threat scenario, the impacts of this actions can be long-term and extensive from the point of view of the time dimension. We have two possible scenarios for this cyber threat. The first of these is the possibility of data being copied under the influence of a second (unwanted) person. This person therefore has a copy of the data at his disposal, just like an employee. The second option is that data is deleted due to an employee's error. In this case, only a person who does not have access to them in the usual way can have the data. In both cases, these data are in the hands of another person. From the point of view of the data owner, this fact cannot be influenced in any way, and therefore the impacts of this action can be long-term, in terms of time.

The physical loss of data represents the last cyber threat, which is rated at degree 5. The impact of the realization of this threat is similar to that of a data leak due to employee negligence. If a carrier of sensitive data and information is lost, these assets can become a powerful tool for extortion or abuse of know-how in the hands of an unauthorized person. Therefore, the longer someone else has this data or information, the greater the impact this fact can have on the organization and its functioning.

The fourth step is to perform a risk analysis in order to express the interaction of individual cyber threats with defined endangered elements. Expression of the interaction of these three indicators was carried out on the basis of the design of the risk matrix. In this risk matrix, selected cyber threats and their assigned values were compared with the endangered elements of the organization's information environment and their values. If there was an interaction between these two indicators (which was not always the case), a value was determined that expressed the degree of vulnerability of the endangered element to a cyber threat. A scale from 1 to 5 was again used to determine the interaction between a cyber threat and a given endangered element, with number 5 indicating the most likely interaction between a cyber threat and a given endangered element, and number 1 the least likely interaction between a cyber threat and a given endangered element. In the following table we can see the individual degrees of risk (Table 6). To better express the degree of risk, each level is assigned a color resolution.

Table 6. Levels of risk (own resource).

Risk	Value Range	Color
Low risk	1–200	
Moderate risk	201–400	
High risk	401–625	

The next step is to create a risk chart in which the probability of the threat, the value of the endangered element, the vulnerability of the endangered element to cyber threats and the time frame of cyber threat, are expressed. As we can see, Figure 4 shows the level of risk for selected cyber threats. The level of risk is always colored according to the proposed scale. The resulting values, which are presented in the graph, are the average values of all interactions between cyber threat and endangered elements. The values of these interactions are obtained on the basis of mathematical Formula (1), in which the probability of a cyber threat, the value of an endangered element (impact), the vulnerability

of an endangered element to cyber threats and the time frame of the cyber threat (degree) are multiplied. Yellow colour signs of a medium level of cyber threat risk. Compared to that a green colour signs a low risk level of cyber threat risk.

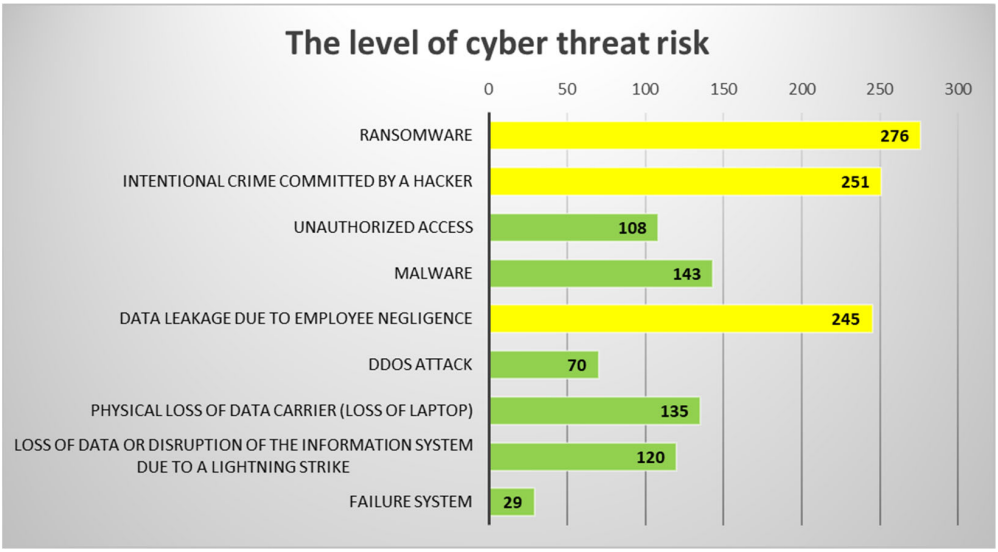

Figure 4. The level of cyber-threat risk (own resource).

The last step of the proposed algorithm is to identify the most serious scenario of a cyber threat, and to financially express the possible impacts of this threat on the information environment of the organization. To achieve this goal, the Saaty method is applied here. The following table is provided to use this method and express the preferences of the individual criteria (Table 7).

Table 7. Criteria and their preferences (own resource).

Number of Points	Descriptor
1	The criteria are equally reciprocal
3	The first criterion is slightly more important than the second
5	The first criterion is more important than the second
7	The first criterion is demonstrably more important than the second
9	The first criterion is absolutely more important than the second

The result of this step is to obtain the upper-right triangular part of the matrix of magnitudes of preferences (sometimes this matrix is also referred to as the Saaty matrix, or the matrix of relative importance). If we denote this matrix by S, then its other elements (on the diagonal and in the lower-left triangular part), are obtained according to the relations:

$$S_{ii} = 1 \qquad \text{for all i,} \tag{10}$$

$$S_{ji} = 1/S_{ji} \qquad \text{for all i and j,} \tag{11}$$

The following table compares selected cyber-threat scenarios with the highest level of risk in terms of impact and financial losses in the vulnerability matrix (Table 8). The purpose of this analysis is to identify one of the most serious cyber threats that can have the greatest impact on an organization and its information system.

Table 8. Cyber threats and determining their significance (own resource).

Cyber Threat	Ransom Ware	Intentional Crime Committed by a Hacker	Data Leakage due to Employee Negligence	Geometric Mean
Ransomware		3	1	1.73
Intentional Crime Committed by a hacker			5	5
Data leakage due to employee negligence				

We determine the values of the criteria weights using the geometric mean of the rows of the Saaty matrix (these values are given in the last column). If we standardize these line geometric means, we obtain the standardized weights of our set of criteria.

$$V_i = G_i / \sum^n G_i \quad (12)$$

where:

V_i = standard weight of the i-th criterion;
G_i = geometric mean of the i-th criterion;
n = number of criteria.

From the results of the analysis carried out by the Saaty method, it can be identified that the most serious threat that can have the greatest impact on the organization is intentional crime committed by a hacker.

The next step is to express the financial impact on the organization and its information environment, which is characterized by defined endangered elements. For the purpose of expressing financial damage, an evaluation scale will be used, which is based on the vulnerability matrix, which was presented in the previous steps. Financial damages are calculated here, and are shown in Table 9.

Table 9. Threat-severity classification (own resource).

The Degree of Severity of the Threat	Percentage of Total
201–220	10
221–240	20
241–260	30
261–280	40
281–300	50
301–320	60
321–340	70
341–360	80
361–380	90
381–400	100

The table shows the severity levels of the threat, which is based on the range of the most serious risks, and is listed in the chart for the level of cyber threat. Based on the achieved results, a scale for the level of medium risk is proposed. No cyber threat was achieved at the highest risk in this case study. The minimum value that can be achieved is 201 and the highest that can be assigned in this risk category is 400. The procedure for determining the degree of severity is as follows:

(1) In the graph of level of cyber-threat risk, the threat that was identified using the Saaty method analysis as the most serious, is selected;
(2) For this threat, the sum of all values that appear in the given matrix is performed (i.e., the interaction of the endangered element and the threat);
(3) The total is divided by the number of interactions;

(4) The value obtained by this mathematical operation is assigned a range of values in the table, with the appropriate percentage;
(5) This percentage is calculated from the amount that was determined at the beginning of the whole process, i.e., the valuation of the organization;
(6) The resulting amount should cover the costs and financial damages that may be caused by this cyber threat.

Calculation:
The sum of the values for cyber threats "intentional committed by a hacker": 4784.
Number of interactions (endangered element × threat): 19.
The average threat value: 4784/19 = 251.
The above table shows that the damage that can be caused by this cyber threat should be 30% of the total amount that can be awarded to the organization and its information. In this case, this amount is EUR 3,713,921 * 0.30 = 1,114,176 Euro.

5. Discussion

The mathematical formula, which was applied in the process of determining the financial impacts of selected cyber threats, was designed based on the relationship between the level of risk and its potential impact. This mathematical formula was extended to include the vulnerability of endangered elements to cyber threats and the time frame. Our findings show that if we consider only its probability and impact when determining the implementation of a cyber threat, this approach is not very suitable for the needs of the insurance industry (Piromsopa et al. 2017). Other factors are important in the process of determining the risk of cyber threats and the other possible related financial impacts. These are, for example, the elements that may be most affected by the impact of cyber threats (Maurya et al. 2018). The proposed elements were identified in our research on the basis of an analysis of the available literature, which is focused on this issue (Romanosky et al. 2019; Sharbaf 2019; Srinidhi et al. 2015).

Interviews and discussions with experts in the fields of insurance, economics, cyber security, digital technologies and law also had an important role in the process of identifying vulnerable areas. Based on this research, we have identified endangered elements (areas) in which organizations can suffer major financial damage. The endangered elements could be extended to other areas in the future. Another area that can have a significant impact on the process of cyber threats and their potential impacts is the time frame. The cyber threat can have different durations, and thus dynamically change its possible financial impacts.

For our purposes, we have compiled five different levels, which are designed based on the correlation between the cyber threat and its duration. It must be taken into account that predicting the evolution of cyber threats over time is a very complex process. Due to the fact that cyber threats take place in most cases in the digital environment, it is very difficult to model their possible future process and development (Naghizadeh and Liu 2014). However, it is very important to include this fact in our algorithm. If we considered only the probability, impact and endangered elements in this process, the results achieved would only be static. In order to determine the possible financial impacts more precisely, it seems appropriate to also include the dynamic development of cyber threats, which represents a time frame in the proposed algorithm.

6. Conclusions

In the research and case study, we described and presented an algorithm for expressing the potential financial impacts of selected cyber threats. This area was researched on the basis of a search and analysis of the insurance sector, which provides insurance to compensate for the impacts of cyber threats. The basic research was conducted as part of the dissertation of one of the authors. During the research, it was found that cyber-threat insurance is a new transdisciplinary area, and that interest in this type of insurance is growing (PWC 2015). The COVID-19 pandemic also made a significant contribution to this fact. During this pandemic, there was a multiple increase in cyber threats, especially on

strategically important objects. Based on the achieved results, it can also be stated that the correct assessment of cyber threats is a key activity of the entire insurance process.

Actuarial mathematical methods are currently used, which are very beneficial from the point of view of insurance and mathematical calculations; however, the issue of information systems or security does not enter into this process (Chaisiri et al. 2015). In order to more accurately express potential damages to the organization's information environment, it is necessary to include these facts in the process of determining the insurance value. This hypothesis is also supported by the current professional community which deals with this issue. The procedures and mathematical methods currently used in insuring organizations against cyber threats do not form a comprehensive algorithm or methodology. As the development has progressed, insurance pricing models have also developed, although advanced pricing based on verified historical data and actuarial models in the field of cyber-threat insurance has not yet been sufficiently verified (Thomas and Finkle 2014; The Lawyer 2010; Toregas and Zahn 2014).

The application of the algorithm that was proposed in this paper allows, unlike other methods, the determination of a specific financial amount (compared with cyber value-at-risk). This financial amount should reflect the possible financial impacts caused by the realization of a cyber threat. The proposed algorithm also includes the assessment of endangered elements, on the basis of which it is possible to determine the amount of potential financial damages. The algorithm also includes risk analyses, taking into account the interaction of cyber threats with endangered elements. It is therefore a combination of approaches that are extended by our own methods of risk analysis and pricing methods. These new methods enable the achievement of results that are based on a more comprehensive analysis of the organization's information environment. The algorithm has also been extended to include the time frame, which can provide a new perspective on estimating the course and impact of cyber threats (compared with the FAIR method).

In our opinion, insurance against cyber threats, together with insurers, should primarily contribute to the protection of the information environment of organizations against liquidation damages, comprehensively and in accordance with the given risk situation. Based on the findings, it can be stated that in the field of insurance, existing procedures to determine the amount of economic impact on the organization in terms of cyber threats need to be improved. It was therefore necessary to create an algorithm that would allow the determination of the insurance value resulting from the impacts of selected cyber threats on the organization from the perspective of the insurance industry. The main benefit of the proposed algorithm is an expression of the financial value of the endangered elements of the organization, which are the areas of the information environment that may be most affected by the impact of the cyber threat. Furthermore, it allows for the modeling of the impacts of a selected cyber threat, which may cause the most serious financial damage to the monitored endangered elements of the organization. The result of this process is also the determination of the optimal insurance value.

Author Contributions: Conceptualization, L.P.; methodology, M.F.; software, L.P.; validation, J.R.; formal analysis, J.R.; investigation, L.P.; resources, L.P.; data curation, M.F.; writing—original draft preparation, L.P.; writing—review editing, M.F. and J.R.; visualization L.P. and M.F.; supervision, L.P.; project administration, J.R.; funding acquisition, L.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Tomas Bata University in Zlín (RVO/FLKŘ/2022/03).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Notes

[1] The coefficient in the first year is determined on the basis of the applicable legislation for a specific state, which deals with income tax.

[2] The coefficient valid in the coming years is determined on the basis of the applicable legislation for a specific state that deals with income tax.

References

Aldasoro, Iñaki, Leonardo Gambacorta, Paolo Giudici, and Thomas Leach. 2020. *Operational and Cyber Risk Measurement in the Financial Sector*. Bank for International Settlements Working Paper (BIS Working Papers), 840. Basel: Bank for International Settlements.

Bahşi, Hayretdin, Ulrik Franke, and Even Langfeldt Friberg. 2019. The cyber insurance market in Norway. *Information and Computer Security* 28: 54–67. [CrossRef]

Bandyopadhyay, Tridib, Vijay S. Mookerjee, and Ram C. Rao. 2009. Why it managers don't go for cyber-insurance products. *Communications of the ACM* 52: 68–73. [CrossRef]

Biener, Christian, Martin Eling, and Jan Hendrik Wirfs. 2015. Insurability of cyber risk: An Empirical analysis. *The Geneva Papers on Risk and Insurance-Issues and Practice* 40: 131–158. [CrossRef]

Böhme, Rainer. 2010. Security metrics and security investment models. In *Advances in Information and Computer Security (IWSEC): 5th International Worshop on Security, IWSEC 2010, Kobe, Japan, 22–24 November 2010*. Berlin and Heidelberg: Springer, pp. 10–24.

Bradford, Josh. 2015. Advisen Insight Cyber Insurance Market Update. Available online: http://www.advisenltd.com/2015/01/15/advisen-insight-cyber-insurancemarket-update (accessed on 8 July 2022).

Chaisiri, Sivadon, Ryan K. L. Ko, and Dusit Niyato. 2015. A joint optimization approach to security-as-a-service allocation and cyber insurance Management. Paper presented at IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Helsinky, Finland, August 20–22; pp. 426–433.

Czech Association of Insurance Companies. 2022. Glossary. Available online: https://www.cap.cz/slovnik-pojmu?start=50 (accessed on 3 May 2022).

Eling, Martin, and Jan Hendrik Wirfs. 2016. *Cyber Risk: Too Big to Insure? Risk Transfer Options for A Mercurial Risk Class*. St. Gallen: University of St. Gallen, Institute of Insurance Economics, pp. 1–163.

Erola, Arnau, Ioannis Agrafiotis, Jason R. C. Nurse, Louise Axon, Michael Goldsmith, and Sadie Creese. 2022. A System to Calculate Cyber Value-at-Risk. Available online: https://www.sciencedirect.com/science/article/pii/S0167404821003692?via%3Dihub (accessed on 14 July 2022).

European Insurance and Occupational Pensions Authority. 2019. Cyber Risk for Insurers—Challenges and Opportunities. Available online: https://www.eiopa.europa.eu/sites/default/files/publications/reports/eiopa_cyber_risk_for_insurers_sept2019.pdf (accessed on 22 June 2022).

Farnan, Oliver J., and Jason R. C. Nurse. 2016. Exploring a controls-based assessment of infrastructure vulnerability. Paper presented at International Conference on Risks and Security of Internet and Systems, Roscoff, France, September 5–7. Berlin and Heidelberg: Springer, pp. 144–159.

Franke, Ulrik. 2017. The Cyber Insurance Market in Sweden. *Computers & Security* 68: 13–144. Available online: https://www.sciencedirect.com (accessed on 10 May 2022).

Giudici, Paolo, and Emanuela Raffinetti. 2022. Explainable AI methods in cyber risk management. *Quality and Reliability Engineering International* 38: 1318–26. [CrossRef]

HM Government & Marsh Ltd. 2015. UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk. Available online: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415354/UK_Cyber_Security_Report_Final.pdf (accessed on 3 August 2022).

Hofmann, Annette. 2007. Internalizing externalities of loss prevention through insurance monopoly: An analysis of interdependent risks. *Geneva Risk and Insurance Review* 32: 91–111. [CrossRef]

Kaspersky Lab ICS CERT. 2018. Threat Landscape for Industrial Automation Systems. Available online: https://ics-cert.kaspersky.com/reports/2019/03/27/threat-landscape-for-industrial-automation-systems-h2-2018/#_Toc4416091 (accessed on 22 July 2022).

Krautsevich, Leanid, Fabio Martinelli, and Artsiom Yautsiukhin. 2011. Formal analysis of security metrics and risk. Paper presented at IFIP Inter-national Workshop on Information Security Theory and Practices, Heraklion, Crete, Greece, June 1–3; pp. 304–19.

Thomas, Leigh, and Jim Finkle. 2014. Insurers Struggle to Get Grip on Burgeoning Cyber Risk Market. Available online: https://www.reuters.com/article/us-insurance-cybersecurity-idUSKBN0FJ0B820140714 (accessed on 17 August 2022).

Lin, Zhaoxin, Travis R. A. Sapp, Rahul Parsa, Jackie Rees Ulmer, and Chengxin Cao. 2022. Pricing Cyber Security Insurance. *Journal of Mathematical Finance* 12: 46–70. [CrossRef]

Majuca, Ruperto P., William Yurcik, and Jay P. Kesan. 2006. The evolution of cyberinsurance. *arXiv* arXiv:cs/0601020.

Marotta, Angelica, Fabio Martinelli, Stefano Nanni, Albina Orlando, and Artsiom Yautsiukhin. 2017. Cyber-insurance survey. *Computer Science Review* 24: 35–61. [CrossRef]

Marsh Insights. 2015. UK Cyber Risk Survey Report. Available online: http://uk.marsh.com/Portals/18/Documents/UK%202015%20Cyber%20Risk%20Survey%20Report-06-2015.pdf (accessed on 11 May 2022).

Martinelli, Fabio, Albina Orlando, Ganbayar Uuganbayar, and Artsiom Yautsiukhin. 2017. Preventing the drop in security investments for non-competitive cyber-insurance market. Paper presented at 12th International Conference on Risks and Security of Internet and Systems (CRISIS), Dinard, France, September 19–21. pp. 19–21.

Maurya, A. K., Neeraj Kumar, Alka Agrawal, and Raees Ahmad Khan. 2018. Ransomware Evolution, Target and Safety Measures. *International Journal of Computer Sciences and Engineering* 5: 68–73. [CrossRef]

Meland, Per Håkon, and Fredrik Seehusen. 2018. When to treat security Risks with cyber insurance. *International Journal on Cyber Situational Awareness* 3: 39–60. [CrossRef]

Millaire, Pascal, John Farley, Sarah Stephens, Stuart Kohn, Paul Nikhinson, Mary Guzman, and Sudhir Bhatti. 2018. Latest Industry Trends in Cyber Security and Cyber Insurance. Available online: https://insights.cybcube.com/en/latest-industry-trends-in-cyber-security-and-cyber-insurance (accessed on 17 June 2022).

Naghizadeh, Parinaz, and Mingyan Liu. 2014. Voluntary participation in cyber-Insurance markets. Paper presented at Workshop on the Economics of Information Security (WEIS), State College, PA, USA, June 23–24; pp. 251–62.

Palsson, Kjartan, Steinn Gudmundsson, and Sachin Shetty. 2020. Analysis of the impact of cyber events for cyber insurance. *The Geneva Papers on Risk and Insurance—Issues and Practice* 45: 564–79. [CrossRef]

Pavlík, Luká. 2019. Design Methodology for Determining the Financial Damage caused by Cyber Threats in the Field of Insurance. Paper presented at International Conference on Military Technologies (ICMT), Brno, Czech Republic, May 30–31; pp. 1–7.

Piromsopa, Krerk, Tomas Klima, and Lukas Pavlik. 2017. Designing model for calculating the amount of cyber risk insurance. Paper presented at IEEE International Conference on Mathematics and Computers in Sciences and Industry, Corfu, Greece, August 24–27; pp. 327–33.

Ponemon Institute. 2017. Cost of Data Breach Study—Global Overview. Available online: https://www.ncsl.org/documents/taskforces/IBM_Ponemon2017CostofDataBreachStudy.pdf (accessed on 13 July 2022).

PWC. 2015. Insurance 2020 & Beyond: Necessity Is the Mother of Reinvention. Available online: //www.pwc.com/gx/en/insurance/publications/assets/pwc-insurance-2020-and-beyond.pdf (accessed on 15 August 2022).

Romanosky, Sasha. 2016. Examining the costs and causes of cyber incidents. *Journal of Cybersecurity* 2: 121–35. [CrossRef]

Romanosky, Sasha, Lillian Ablon, Andreas Kuehn, and Therese Jones. 2019. Content analysis of cyber insurance policies: How do carriers price cyber risk? *Journal of Cybersecurity* 5: 1–38. [CrossRef]

Schwartz, Mathew J. 2019. Ransomware: Average Ransom Payout Increases to $41,000. Available online: https://www.bankinfosecurity.com/ransomware-average-ransom-payout-increases-to-41198-a-13333 (accessed on 30 June 2022).

Sharbaf, Mehrdad. 2019. Reengineering Cyber Security Process: A New Perspective on Cyber Security Quality Management. Paper presented at IEEE International Conference on Dependable, Fukuoka, Japan, August 5–8; pp. 332–37.

Shetty, Nikhil, Galina Schwartz, Mark Felegyhazi, and Jean Walrand. 2010. Competitive cyber-insurance and internet security. Paper presented at Workshop on the Economic of Information Security (WEIS), London, UK, June 24–25; pp. 229–47.

Siegel, Carol A., Ty R. Sagalow, and Paul Serritella. 2002. Cyber-risk management: Technical and insurance controls for enterprise-level security. In *Information Security Management Handbook*. Boca Raton: Auerbach Publications, vol. 4, pp. 433–49.

Srinidhi, Bin, Jia Yan, and Giri Kumar Tayi. 2015. Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors. *Decision Support Systems* 75: 49–62. [CrossRef]

The Lawyer. 2010. Incentives and Barriers of the Cyber Insurance Market in Europe. Available online: https://www.thelawyer.com/issues/13-september-2010/as-professional-indemnity-crisis-rumbles-on-the-sraconsults/ (accessed on 25 May 2022).

Toregas, Costis, and Nicolas Zahn. 2014. Insurance for Cyber Attacks: The Issue of Setting Premiums in Context. Available online: https://cspri.seas.gwu.edu/sites/g/files/zaxdzs4106/f/downloads/cyberinsurance_paper_pdf_0.pdf (accessed on 23 August 2022).

Woods, Daniel, and Andrew Simpson. 2017. Policy measures and cyber insurance: A framework. *Journal of Cyber Policy* 2: 209–26. [CrossRef]

Woods, Daniel, Ioannis Agrafiotis, Jason R. C. Nurse, and Sadie Creese. 2017. Mapping the coverage of security controls in cyber insurance proposal forms. *Journal of Internet Services and Applications* 8: 526–34. [CrossRef]

Young, Derek, Juan Lopez Jr., Mason Rice, Benjamin Ramsey, and Robert McTasney. 2016. A framework for incorporating insurance in critical infrastructure cyber risk strategies. *International Journal of Critical Infrastructure Protection* 14: 43–57. [CrossRef]