International Scientific Conference
CONTEMPORARY ISSUES IN BUSINESS, MANAGEMENT AND ECONOMICS ENGINEERING 2021
13–14 May 2021, Vilnius, Lithuania
Vilnius Gediminas Technical University
eISSN 2538-8711
eISBN 978-609-476-260-4
Article ID: cibmee.2021.618
https://doi.org/10.3846/cibmee.2021.618

FORECASTING COSTS OF CYBER ATTACKS USING ESTIMATION THE GLOBAL COST OF CYBER RISK CALCULATOR V 1.2

Julija GAVĖNAITĖ-SIRVYDIENĖ, Algita MIEČINSKIENĖ*

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

Received 28 February 2021; accepted 01 April 2021

Abstract. *Purpose* – due to the constant increase of cyber-attacks not only the measures of identifying and controlling cyber risks are created, but also the methods of estimating possible cyber-attacks financial costs should be developed to increase business preparedness. The purpose of this research is to forecast potential costs of cyber-attacks in Baltic countries.

Research methodology – to achieve the aim of the article and prepare a prognosis of possible cyber-attacks costs the *Estimation the Global Costs of Cyber Risk Calculator V 1.2* tool was used.

Findings – estimated costs of cyber-attacks in Lithuania, Latvia and Estonia are highest in the public business and services sector and also in the defense sector. According to conducted calculations the costs of cyber-attacks in Lithuania will reach 1% of GDP of Lithuania by 2026.

Research limitations – in this research the costs of cyber-attacks are estimated regarding industries of business but not excluding specific cyber threats. Therefore, for the future research possibilities could be the analyses of specific cyber risks and their impact to various business sectors.

Practical implications – the results of the research may be useful in practical approach for preparing the risk management tools, evaluating possible damage and effect of cyber-attacks to business, also increasing preparedness level and business resilience.

Originality/Value – this estimation model has been not used to evaluate and discuss cyber-risks costs in Lithuania among previous researches, therefore the topic and conducted results are original and significantly relevant for further analyses of cyber security issues in Lithuania.

Keywords: cyber-attack, cyber security, cyber costs, cyber risk management, forecasting.

JEL Classification: C53, G32.

Conference topic: Contemporary Financial Management.

Introduction

Institutions of various magnitude, business type or location globally have been affected by consequences caused of cyber-attacks regarding financial, operational, reputational or other fields. During past few years, a significant rise in cyber risk exposures were captured in different sectors. Generally, cybersecurity is fast improving and cyber resilience of businesses is growing, but beside that attackers are also continuously evolving their techniques, changing key target tactics and shaping different models of cyber-attacks. New cyber security legal requirements target to keep companies and their management boards more responsible in the security of information or data assets and IT infrastructure. The General Data Protection Regulation (GDPR) have been affective since May 25, 2018 with indicated fines possibly exceeding to €20 million or four percent of annual global revenues (European Parliament and the Council, 2016). Since the regulation took effect, the French data regulator (CNIL) issued the largest GDPR fine so far – €50 million. Constantly, businesses have to cope with an everchanging and evolving risk landscape, which has been further increased by the outbreak of the coronavirus pandemic.

Organizations are encountered by a number of different challenges, such as the possibility of more complicated and expensive business interruptions, the increase in the frequency and cost of cyber-attacks, the critical consequences

*E-mail: *julija.gavenaite@gmail.com*

© 2021 Authors. Published by Vilnius Gediminas Technical University. This is an open-access article distributed under the terms of the Creative Commons Attribution (http://creativecommons.org/licenses/by/4.0/) License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

of large sensitive data leaks and stricter regulations. Related to the changes in working environment (remote work), new possibilities for cyber criminals, who are becoming more sophisticated and using more developed methods, to obtain access to private databases, sensitive information or internal networks, are growing every day. Also, the possible effect from human error or IT distortions occurrences become one of the most relevant indicators of cyber risks. Therefore, employers and employees increase general appreciation and cyber resilience in the context of changed working environment.

Regarding of the variety of sensitive or personal data, financial information and resources that business and institutions are in possession of, they are facing an aggressively growing pressure from cyber-attacks. Those risk came in very different forms and channels, and in relation to changed business environment usually are harder to predict and identify. The major reason for the significance of cyber security is to secure all the customer personal data and assets together with business continuity and internal assets safety. Therefore, it is highly important for institutions to implement cyber security programs, take all possible actions of prevention and to establish the plan for investments in cyber security. Moreover, the consequences of cyber-attacks, such as personal data or financial credentials leakage may be critically significant not only for reputational matter but also for company's financial stability and business continuity.

Cyber-attacks have resulted in significant financial and non-financial losses because of the increasing frequency and costs. Relevant forecast of cyber losses could be a very useful tool for companies to evaluate their business preparedness, invest in cyber security and prevent business from interruptions.

The purpose of the research: due to the constant increase of cyber-attacks not only the measures of identifying and controlling cyber risks are created, but also the methods of estimating possible cyber-attacks costs should be developed to increase business preparedness. The aim of this paper is to forecast possible costs of cyber-attacks in Lithuania.

Research methodology: to achieve the aim of the article and prepare a prognosis of possible cyber-attacks costs the Estimation the Global Costs of Cyber Risk Calculator V 1.2 tool was used. Also, these methods for scientific research were used: comparative data analyses, data modeling, analyses of statistical data.

The structure of the paper: this paper contains three main parts. First part is dedicated for cyber security concept, discussing different approaches proposed by various researches and indicating general issues regarding cyber security. Also, the first part involves the overview of conducted researches on the estimation of cyber-risk costs. In the second part of the paper the methodology for estimating cyber security costs is presented and explained. The final third part includes the results of cyber costs evaluations and gives final conclusions on the topic.

1. Cyber security concept

Cyber security term has been the subject of scientific researches that has largely reviewed the topic from various perspectives. The definitions of cyber security or cyber risk are highly variable and diverse. Fredrick Chang (2012), former Director of Research at the National Security Agency in the USA suggest the interdisciplinary concept of cybersecurity describing it as a field of science that offers a variety of possibilities for advances based on a multidisciplinary attitude, thus, after all, cybersecurity is fundamentally about a competition and involvement. Humans must defend machines that are attacked by other humans using machines. So, additionally to the critical traditional fields of IT science, electrical engineering, and mathematics, perspectives from other fields are needed. According to DHS (2014) cyber security can be described as the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are secured from and/or defended against disruptions, illegal use or changes, or exploitation. Oxford Academic Journal of Cyber Security (Brantly, 2021) suggests that cyber security shall be considered as a state of being protected from unauthorized use or access, criminal intervention or the measures that are taken to avoid these situations. According to (Advisen, 2018), cyber security may be defined as a process of protecting all electronic devices and online storage (computers, mobile devices, servers, electronic systems, networks, online data and clouds storage) from cyber-attacks.

In particular, describing concept of cybersecurity, these general features and indications are provided (Chang, 2012):

1. the possibility to secure or defend the business environment from cyber-attacks;
2. prevention of integrity, accessibility of information confidentiality in the business environment;
3. all measures and activities supposed to be intended for users and cyber space protection;
4. prevention of risk and possible damage in purpose to protect and if necessary, restore information, data, online storage, electronic communication systems and services.

Figure 1 represents a schematic approach of the cybersecurity concept. It can be indicated that cyber security targets at securing the cyberspace (which includes both software and hardware) from any cyber threat or cyber-attack. The attitude and actions related with cyber-security management actions followed by businesses and counties to pro-

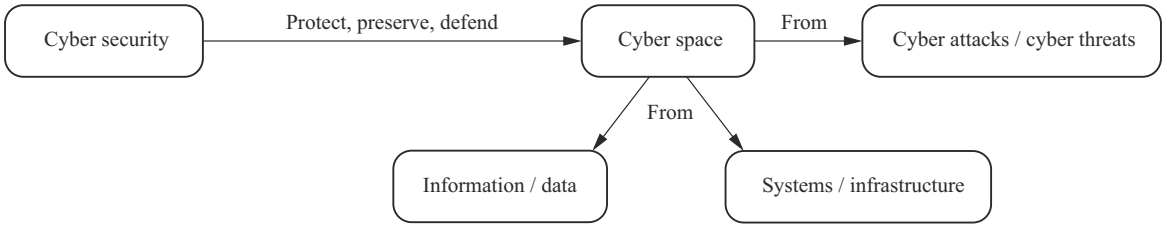

Figure 1. Definition of cyber security
(source: compiled by author, based on Chang, 2012; Advisen, 2018)

tect confidentiality, integrity and approachability of software information and hardware used in cyber space (Schatz er al., 2017). The conception involves guidelines, requirements and collections of safeguards, technologies, tools and training of employees to provide the best protection for the company's cyber space and its consumers.

To summarize the description and concept of cyber security general components may be excluded:

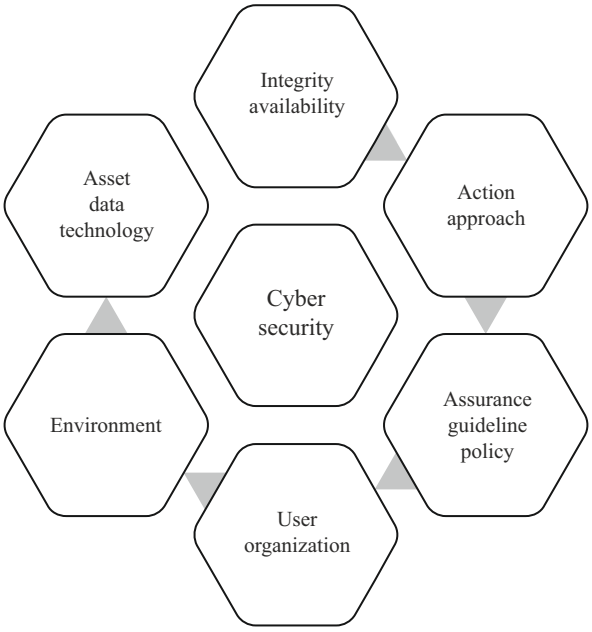

Figure 2. Cyber security layers
(source: compiled by author based on Schatz et al., 2017)

The Figure 2 presents the underlying concepts of cyber security that involves different dimensions: integrity/availability – implies how important and necessary to reach any tools, information and data; action/approach – represents company's' protocol or strategy on cyber security and cyber risks management; assurance/guideline/policy – important parts of cyber security concept that involves detailed information and tools for dealing this cyber risks; user/organization – represents human capital of this concept; environment – this may be business environment; the industry that company is operating in, cyber security environment; asset/data/technology – refers to all the hardware and software that supposed to be protected from cyber risks.

Cybersecurity refers to a link between different indicators such as measures of risk evaluation, methodologies for risk management, skills and policies to reach the general target – improvement of asset, sensitive information or data security. Moreover, the important part is to ensure that the feedback about the confidentiality, availability and compliance of information is gathered and provided to responsible institutions (Cavelty, 2018). An efficient strategy for cybersecurity requires a high-level engagement of all accountable elements in the organization.

Regarding the classification of cyber risks there a variety of different approaches proposed in scientific literature, but these common types are identified:

1. Classifying cyber risks regarding the source (network; hardware; application) or regarding the target or the possible attack (to steal sensitive information, to take-over a control of application, to track and exfiltrate data) (Toch el al., 2018);
2. Dividing cyber risks into groups according to the reason of cyber incident (human mistake, failures of systems or devices, inaccuracy among internal processes, external issues) (Chapelle et al., 2018);

3. Types of cyber risks in the context of attack methods (ransomware, hacking, malware, malicious code, social engineering or phishing, denial of services) (Wu et al., 2015).

Generally, all these classification approaches suggests that cyber risks are characterized by the source of attack (external, internal, human mistake) or by the instrument that is applied to attempting cyber-attack. Despite the differences among these approaches all of them concludes to the same outcome – the danger or damage for sensitive data, information, IT infrastructures or assets.

2. Overview of researches on estimating global costs of cyber-attacks

Cyber-attacks have resulted in a very significant financial and non-financial losses because of the increasing frequency and cost in past years. There can be found a variety of scientific researches and studies to evaluate systemic and also direct cost of cyber-attacks, that can be analyzed and considered across different business sectors, industries and regions (Allianz Global Corporate, 2019). Despite the variety of studies, most of them are based on a very different measures and tools, for example – annual costs, costs per sector, costs per attack. Because of the different measurement approach, usually results of estimations and forecast are inconsistent.

According to British national organization called Home Office Science Advisory Council [HOSAC] (2018), a quality of data and forecasting models should be improved. Building a wider and better understanding of cyber costs is crucial to:

- Better understanding the nature of cyber threats and how they are evolving over time;
- Building the awareness of cyber security and cyber costs significance in order to empower of making relevant decisions;
- Activating and directing appropriate level of awareness and risk management initiatives towards business who are most vulnerable and affected by costs of cyber-attacks.

According to CyberSecurity Ventures (2020), one the leading researches for global cyber security, the costs of cybercrimes are expected to grow by 15 percent per year over the following five years and to reach 10.5 trillion of USD dollars annually by 2025. This cyber cost estimation was based on historical cybercrimes figures collected globally, together with year-over-year growth and comparison, organized cybercrime activities statistics from governmental institutions. Cybercrime costs involves destruction and damage to data, lost productivity, stolen money and other alternative financial resources, theft of intellectual property, stolen sensitive personal information and financial accounts, fraud and also post attack disruption that the company may be facing. Moreover, the investigation, restoration and other cyber security management improvements must be calculated in.

There is a number of reasons why forecasting possible costs of cyber-attacks can be difficult. First of all, cyber costs may possible be under evaluated because there is a lack of accurate and reliable information. Organizations that experienced cyberattacks possibly are indisposed to report or give more details about the cyber-attacks or possibly the reported information may be incomplete, without fully estimating the indirect costs that are experienced because of the breach. Also, cyber-attacks costs that are a result of third-party breach are harder to predict and asses (Ponemon Institute, 2018). Moreover, some of the costs are difficult to quantify, especially for the larger dimension impacts on financial stability, consumer confidence or business reputation. For instance, losses related with reduced investment or consumption due to increased uncertainty of cyber risk can be significant, but hard to evaluate. Cyberattacks could also affect the layout of innovation or investments by reducing the expected return to innovators and investors or profit margins. Moreover, there is a type of possible costs that arises as not implemented or only partly used benefits of information technologies and these costs can hardly be fully forecasted (National Institute of Standards and Technology, 2018). Lastly, possible cyber costs continue to increase as more business functions move online, more people connect to the internet globally, and more essential services are provided by third parties online. The significant scale of global digitalization leads to the problem, that historical data that are used for forecasting possibly not be relevant and efficient for presuming future indications and projecting possible future cyber costs trends.

Deloitte suggested a method that could be used as a tool for cyber cost estimation in 2013. This method uses the ratio between the cost of cyber risk and total income obtained as an empirical data. It is based on different data collected for a wide range of businesses and financial corporations over different industries. Data collection is for tracking levels, types, occurrence frequencies of cyber-attacks together with types of assets, profiles or data that is attacked. The general process of this method created a connection between costs of cyber risks occurrence and general income by the industry (Deloitte, 2018). Basically, this method produces two parameters: the possible loss valuation for each $1billion of earnings in the industry, and a Value at Risk (VaR) measure which evaluates the higher area of losses in a given period of time (in this case, over a year) at the 95% confidence level (Ruith & Spatary, 2016). Though, in cyber-risk context, Value at Risk model has limitations because of the accessibility of historical data, software vulnerabilities identification and the limited risk scenarios it can be supported and well used for obtaining insights.

To summarize, due to privacy concerns, assumptions, and data sources, reporting on cyber-attacks costs seems to move toward anonymization, and because of that it is severe to ensure clarity in the research models. In addition, it

is found that the majority of researches in this topic concentrates on direct or indirect costs to the organization; there was rather less discussions and reviews on the macroeconomic level effects faced by different sectors as of the focus on direct costs by different industries.

3. Methodology for modeling the Costs of Cyber-attacks with The Global Cost of Cyber Risk Calculator V 1.2

The cyber costs estimation tool called *Global Cost of Cyber Risk Calculator* was suggested by Drayer et al. (2018) and the purpose of this analyzed tool is to provide a model for evaluating instant and potential losses caused by cyber-attacks taking into consideration the frequency, uncertainty and different types or sources of potential cyber-attacks.

3.1. Structure of the model

General features and functions of this calculation model are:

1. identify the VaR indicator regarding the business field and geographical area.
2. compute immediate costs by involving various financial situations for each business part and the fraction of every situation that is possibly endangered to cyber threats.
3. compute the systemic costs of cyber-attacks among business sectors using Organisation for Economic Cooperation and Development input, output, and value-added information across industries in more than 60 locations.

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

The created model allows to evaluate the effect that various cyber-attacks have on the value-added gross domestic product (GDP) of business in the region. To construct this model, these criteria's necessary to be indicated:

– Countries: $c \in C$.
– Industry sectors: $i \in I$.
– Economic exposures: $e \in E$.
– Perils: $p \in P$.

A model is constructed with a dimension of countries C, industry sectors I, economic exposures E, and perils P. Thus, every country c is in the dimension of countries C, every industry sector i is in the dimension of industry sectors I, every financial exposure e is in the dimension of economic exposures E, and every peril p is in the dimension of perils P where a cyber- risk occurrence actions on purposes may follow in costs implicated by the defender. Dimensions are implemented as a definition and thus cannot be divided.

Each dimension is described to be substantive of another but may not be both incompatible or comprehensive. The dimension of countries C, for instance, is a sub-dimension of all the countries around the world, and its value depends on information accessibility. The dimension of industry sectors I is also to be described as incompatible or comprehensive. Thus, the dimension of financial exposures E and perils P are indicated to be both mutually exclusive and collectively exhaustive, the over changing nature of cyber-attacks possibly broaden this dimension beyond the descriptions currently within this methodology. Also, the authors of the model presumed additive segregation of direct costs, such that in estimating direct expenditures, sub-dimensions within each dimension do not influence each other but associates among the wider systemic expenditures' estimations.

In the method investigation, it is related cyber-attack losses to GDP loss in a particular sector and industry. This attitude takes into consideration for both rebound results between organizations (where a damage in one organization possibly lead to the benefit in other organization) and lowers the necessity to calculate over a different of broadly uncertain types of damages.

Specifically, costs are divided into:

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

In this context, direct costs involve expenditures that are strictly paid by an industry in any period of a cyber-risk occurrence, involving costs in the configuration of attests, penalties, ravishment and investigation price, and business termination that takes place in the industry that experienced cyber-attack, together with possible lawsuits prices that may be experienced by third parties but are indemnified by the organization that experienced the cyber-attack.

The general outputs of analyzed tool:

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

Basically, this calculator model runs either creates the possible values of the losses provided the general outcomes of the input data, otherwise makes a huge amount of draws on the general outcomes to evaluate the outcome purpose of the losses.

3.2. Direct costs dimension on the sector and country scales

In this model immediate costs to exposure and GDP are calculated for every sector i in country c by concluding the dimensions (c, i, e, and p) to G_c (which is the GDP of country). These moves are followed:

- firstly, w_{ci} is defined as sector i's shares of GDP in country c.
- $w_{ci} * G_c$ is the value added (contribution to GDP) of sector i in country c.
- it is also defined O_{ci} as the sector output of sector i in country c.
- the unitless value Y_{cie} is described to be the fraction of industry sector output that is adequate to the amount of money at risk from every possibility type (e), despite of whether they can be affected by a cyber-attack.
- 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).
- 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.

Based on the provided measurements and connections, it can be determined the immediate cost to sector exposure in every sector i in country c by the sum over the product Y_{cie} and X_{ciep} for all perils p and outcomes e, which, multiplied by the exposure of sector i in country c (O_{ci}), gives the total sector direct costs to exposures as follows:

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

Taking into consideration possible modifications in sector exposure scale to changes in sector GDP, one can closely describe the direct exposures to sector GDP, letting (d), + denote the loss to sector GDP:

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

Moreover, combining sector-level direct costs (d), allows us to evaluate the total direct costs to exposure and GDP from cyber risks for every country c like following:

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

Because of the density of sets and instability in cyber-risk projections, one might intend to evaluate how various method approaches influence the well-understood value of w), $* G$), the GDP of country c that is in sector i. The outcome evaluation possibly relies highly on the inputs of perils, exposures, industries, and their combinations. Thus, indicating sectors and exposures is simple, evaluating the effect of perils on exposures is a highly complicated. Therefore, the method is developed to lay bare the indeterminacy around these inputs by empowering users to change input connections and indicating the effected modifications among the final calculations.

3.3. The future costs projection

This estimation model allows to update any of the dimensions or connections among the dimensions for present or in the future. For instance, it is possible to:

- indicate a specific GDP growth for a period of time.
- use the Organisation for Economic Co-operation and Development (OECD, 2018a, 2018b, 2018c, 2018d) financial estimations set to complete financial estimations overviews for one year of GDP for every country.
- replace predictions of how perils (p) possibly change financial exposures (e).

Above mentioned affects would be implicated through the method to evaluate new costs. In every scenario, the replacements may be pointed as evaluations or can be implied from possibility allocations, affecting in the allocation of possible costs. In the calculator, it is possibility to overview expenses within a region cover a year, with a condition that these general estimations may not be region specified (Drayer, 2016).

Basically, this calculator generates the ordinary suggestion and accomplish a 1% growth in GDP every year for high-income countries, a 6% growth for upper-middle-income countries, and a 7% increase for lower-middle-income countries, according to World Bank (2016) classificatory.

Model Parameters. Various different dimensions of sets in necessity to be indicated for the calculator to forecast. To run the method and approve that calculations, the dimension sets were estimated using data from analyses of the scientific researches and data investigations. The dimensions possibly be either point evaluations or possibility outcomes, and the combination of them possibly provide estimated values and possibility circulations of exposures:

3. *Country* (*C*). Consider that c is determined as a specific country within a dimension of countries, C. According to Ponemon Institute (2019) indicates, the countries and regions presently experiencing high level of cyber-attacks are the United States, the United Kingdom, Germany, Australia, France, Brazil, Japan, Italy, India, Canada, South Africa, the Middle East. Therefore, the method supposed to be supple enough to involve potential

countries at growing risk, this dimension is extended to a wider range (Anderson & Moore, 2018). Due to the fact that the countries are connected to the sectors, a wide range of data dimension that involved information on how industries correlate to country is reached. In the mode, accessible data and financial information gathered by OECD is used.

4. *Industry Sectors* (*I*). Dividing the economy into the sectors is references with a specific sector model according on accessible country-level information, together with the incorporation of data that Deloitte (Jacobs et al., 2013) has introduced as the most significant sectors for cyber-risks. The country-level economic information is based on the Structural Analysis Database. These sectors are aggregated to assimilate the Deloitte sectors of significance.
5. *Financial Exposures* (*E*). Regarding that e is described as the financial outcome among a dimension of financial outcomes, *E*, that could possibly be affected, independent of risk type. These occurrences are deliberated not in their direct relation to GDP, but as a part of production that could possibly be affected by a cyber-attack and could lower the organization's total profit or income. It is established the dimensions of financial outcomes as capital resources, intellectual property (IP), and revenue.
6. *Perils* (*P*). Consider that p is explained as the hazard into the dimension of perils, P, where a cyber attacker's actions on targets may outcome in losses indicated by the organization. Therefore, here a possible dimension that will mostly be renewed. This part is concluded using the various types of sets for event type (Advisen, 2017). Data dimensions includes more than 12,000 cyber-attacks categorized into 5 different entries for occurrence character and 11 different occurrences for occurrence character.

4. Results of the forecasting cyber-attacks costs in Lithuania

The cyber-attacks costs were forecasted using the described *ESTIMATION THE GLOBAL COST OF CYBER RISK CALCULATOR V 1.2* tool (Rand Corporation, 2018). The forecasted period is five years; the results are projected for 2026 and costs of cyber-attacks are expressed in USD dollars.

Forecasted cyber-attacks costs for these business sectors:

1. Banking.
2. Defense and Aerospace.
3. Healthcare and Insurance.
4. Oil, Gas, and Chemicals.
5. Public business and services.
6. Technology and Electronics.
7. Transportation.
8. Utilities and Consumer Goods.
9. Retail.

First of all, the costs of cyber-attacks were forecasted regarding provided list of business sectors and expressing the financial damage to each sector (Table 1). Forecasted results in Lithuania were compared to the results in other Baltic states (Latvia and Estonia).

The forecast results show that the highest cyber-attacks costs are predicted to public business and services sector /defense sectors. The lowest amount of costs is estimated in the banking and technology/electronic business sectors. Generally, it is forecasted that in 5 years the costs of cyber-attacks in Lithuania will reach more than 102 million USD. Also comparing to other Baltic countries (Latvia and Estonia), Lithuania has a highest cyber-attacks costs predicted almost in all industries. This could be motivated by the correlation with general county GDP, IT technology development and investment rate.

Furthermore, the percentage of cyber-attacks costs from the general GDP of the sector in the county was forecasted while comparing the indicated business sectors and countries (Table 2).

Analyzing the results of Lithuania, it can be stated that national defense sector is significantly more vulnerable and exposable to cyber threats than other industries and will have the higher costs from cyber-attacks compared to this sectors GDP. For instance, financial or banking sector is one of the most attractive targets for cyber attackers, but because of the business specific and amount of sensitive and private data companies are possessing and using – cyber risk management is one of the top priorities in banking sector, therefore cyber-attacks possibility is under strict control. As the company's operating in this sector are still in the development stage for cyber security evaluating and management, the investments for risk controls and protection have been low and the regulations are not as strict as for financial and government institutions, business are more vulnerable and exposable for cyber-attacks. The national defense and other governmental institutions in Lithuania have already been facing cyber incidents, such as denial of services, confidential information take over or systems intrusions. Because of the national significance of those institution activity and possessed data the number of potential attacks is anticipated to growth.

Table 1. Forecasted costs of cyber-attacks by 2026 across the industries (million, USD) (source: compiled by author using Global Cost of Cyber Risk Calculator V 1.2)

	Banking	Defense Aerospace	Healthcare Insurance	Oil, Gas, Chemicals	Public business, services	Technology Electronics	Transport	Utilities, Consumer Goods	Retail	TOTAL
LTU	1.75	22.09	0.26	0.38	65.380	1.62	2.67	5.51	2.99	102.65
LV	1.06	13.27	1.15	0.65	65.998	1.527	1.672	0.89	1.91	88.127
EST	0.84	11.947	1.74	2.55	64.456	1.807	1.273	2.612	1.39	8.615

Table 2. Forecasted costs of cyber-attacks by 2026 across the industries (% of sector GDP) (source: compiled by author using Global Cost of Cyber Risk Calculator V 1.2)

	Banking	Defense, Aerospace	Healthcare Insurance	Oil, Gas, Chemicals	Public business, services	Technology Electronics	Transport	Utilities, Consumer Goods	Retail	TOTAL
LTU	0.04%	0.45%	0.01%	0.01%	0.08%	0.10%	0.06%	0.11%	0.06%	0.92%
LV	0.03%	0.43%	0.00%	0.02%	0.15%	0.17%	0.05%	0.09%	0.06%	1.00%
EST	0.04%	0.51%	0.01%	0.01%	0.16%	0.14%	0.05%	0.11%	0.06%	1.09%

Conclusions

Cyber security is one the most relevant and significant issues in relation to ensuring business continuity, general data protection and business environment security.

Depending on the industry and business type, risk channels vulnerable factors, type of sensitive data, information or other assets could become a target of cyber-attack. Organizations operating in different sectors of business have different preparedness level, cyber risk management protocols and general resilience to this type of risk. Therefore, the level of cyber risk exposure is closely related to industry and business or organization type.

Due to legal regulations, guidelines and requirements for reporting the information about experienced cyber-attacks the forecasting of possible cyber costs is complicated in company, business sector and country level. After completing the assessment of cyber cost forecasting approaches, the *Global Cost of Cyber Risk Calculator V 1.2* was acknowledged as a suitable tool for cyber costs forecasting and discussing various economic exposures for every industry.

Regarding the calculation's made there is forecasted that by 2026 cyber-attacks will cost 102.65 million of USD and will reach approximately 0.92% of Lithuania's GDP. The most vulnerable sectors are indicated as public business and services and national defense system. Governmental institutions, especially responsible for national defense have already experienced cyber breaches and interferences. This sector is attractive for cyber attackers because of its sensitivity to general national security, the nature of data and information those organizations are in possess of. Therefore, it is highly possible that the tendency of cyber-attacks in this defense sector will only be growing.

Comparing the results among Baltic countries it is established that in Lithuania the costs of cyber-attacks will be highest and will reach 102.65 million USD compared to 88 million USD in Latvia and Estonia. All three countries share similar values of cyber costs among all the sectors except the defense sector were in Lithuania it is estimated to be about 50% higher that in Latvia and Estonia.

Completed forecast indicates that the lowest costs of cyber-attacks are estimated in the banking sector, oil and chemical producing sector and private healthcare/insurance. Regarding the financial sector and banks situation in the context of possible costs of cyber-attacks it is assumed that low forecast is determined by cyber risk management tools and protocols these sectors are already implementing and investing constantly into online data security, internal and external process supervision and high focus to evolving cyber resilience.

Suggestion for further research regarding the forecasting of cyber-attacks costs is to involve the additional dimensions for example, specific cyber risk parameter regarding business sector. This extension of the research possibly allows to evaluate the damage of different cyber risks regarding type of business and strongly improves the process of cyber risk management.

References

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

Advisen. (2017). *Cyber loss dataset.* https://www.advisenltd.com/data/cyber-loss-data/

Allianz Global Corporate. (2019). *A guide to cyber risk – managing the impact of increasing interconnectivity*.

Anderson, R., & Moore, T. (2018). Information security economics and beyond. In A. Menezes (Ed.), *Lecture notes in computer science: Vol. 4622. Advances in cryptology – CRYPTO 2007*. Springer. https://doi.org/10.1007/978-3-540-74143-5_5

Brantly, A. F. (2021). Risk and uncertainty can be analyzed in cyberspace. *Journal of Cyber Security*, *7*(1), tyab001. https://doi.org/10.1093/cybsec/tyab001.

Cavelty, M. D. (2018). Cybersecurity research meets science and technology studies. *Politics and Governance*, 6(2), 22–30. https://doi.org/10.17645/pag.v6i2.1385

Chang, F. R. (2012). Defining cybersecurity. Guest editor's column. *The Next Wave*, *19*(4), 1–2.

Chapelle, A., Crama, Y., Huebner, G., & Peters, J.-P. (2018). Practical methods for measuring and managing operational risk in the financial sector: a clinical study. *Banking & Finance*, *32*(6). https://doi.org/10.1016/j.jbankfin.2007.09.017

CyberSecurity Ventures. (2020). *Cybercrime to cost the world $10.5 trillion annually by 2025.* Special Report: Cyberwarfare in the C-Suite. Sausalito, California.

Deliberation of the Restricted Committee. (2019). *Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC.*

Deloitte. (2018). *Cyber value at risk in the Netherlands*. https://www.thehaguesecuritydelta.com/images/-deloitte-nl-risk-cyber-value-at-Risk-in-the-Netherlands.pdf

DHS. (2014). *National preparedness goal*; *White House cyberspace policy review.* CNSSI 4009, NIST SP 800-53 Rev 4, NIPP.

Drayer, E. (2016). Resilient distribution grids – cyber threat scenarios and test environment. In *IEEE PES Innovative Smart Grid Technologies Conference Europe* (*ISGT-Europe*). https://doi.org/10.1109/ISGTEurope.2016.7856193

Drayer, P., Jones, T., Klima, T., Oberholtzer, J., Srong, A., Welburn, J., & Winkelman, Z. (2018). *Estimating the global costs of cyber risks.* Justice, Infrastructure and Environment. Rand Corporation.

European Parliament and Council. (2016). *Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC* (*General Data Protection Regulation*).

Home Office Science Advisory Council. (2018). *Understanding the costs of cybercrime*, *a report of key findings from the Costs of Cyber Crime* (Working Group Research Report).

Jacobs, V., Bulters, J., & van Wieren, M. (2013). Modeling the impact of cyber risk for major Dutch organizations. In *Cyber Risk Services*, *European Conference on Cyber Warfare and Security* (pp. 145–154). Deloitte.

National Institute of Standards and Technology. (2018). *Standards for security categorization of federal information and information systems.* FIPS. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

OECD. (2018a). *About the OECD.* http://www.oecd.org/about/

OECD. (2018b). *Brazil – Economic forecast summary* (*November 2017*). http://www.oecd.org/brazil/brazil-economic-forecast-summary.htm

OECD. (2018c). *Input-output tables.* http://stats.oecd.org/Index.aspx?DataSetCode=IOTS

OECD. (2018d). *STAN structural analysis database.* http://www.oecd.org/sti/ind/stanstructuralanalysisdatabase.htm

Ponemon Institute. (2018). *Cost of data breach study: Impact of business continuity management*. IBM. https://www.ibm.com/security/data-breach/

Ponemon Institute. (2019). *Cost of data breach study: global analysis*.

Rand Corporation. (2018). *Global Cost of Cyber Risk Calculator V 1.2* [Computer tool]. https://www.rand.org/pubs/tools/TL281.html

Ruith, J., & Spataru, D. (2016). *The benefits and limits of cyber value-at-risk*. https://deloitte.wsj.com/cio/2015/05/04/the-benefits-limits-of-cyber-value-at-risk/

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. *Journal of Digital Forensics*, *Security and Law*, *12*, 2–8. https://doi.org/10.15394/jdfsl.2017.1476

Toch, E., Bettini, C., Shmueli, E., Radaelli, L., Lanzi, A., Riboni, D., & Lepri, B. (2018). The privacy implications of cyber security systems: A technological survey. *ACM Computing Surveys*, *51*(2), Article 36. https://doi.org/10.1145/3172869

World Bank. (2016). *New country classifications by income level.* https://blogs.worldbank.org/opendata/new-country-classifications-2016

Wu, W., Kang, R., & Li, Z. (2015). Risk assessment method for cyber security of cyber physical systems. In *Proceedings of the 2015 First International Conference on Reliability Systems Engineering* (*ICRSE*) (pp. 21–23). Beijing, China. https://doi.org/10.1109/ICRSE.2015.7366430