Received: 14 April 2020

Accepted for publishing: 6 January 2021

DOI: 10.32025/JBM19003

The challenges of cybersecurity insurance development: The case of Latvia

TATJANA VOLKOVA
LINDA JEKABSONE
ZITA LAVRINOVICA
ELINA SABA
MARIS SABA

ABSTRACT

Purpose. This paper aims to provide an overview of the current challenges of cybersecurity insurance, focusing on the identification of development constraints and opportunities and the key impact factors of this recently emerging insurance market in Latvia.

Methodology. The authors used theoretical and empirical research methods, e.g., a literature review, surveys of experts from principal insurance companies and professionals from prominent mobile network operators, and interviews with experts in cybersecurity and pioneers of cybersecurity insurance in Latvia.

Findings. The research results illustrate the immense difficulties in providing cyber risk insurance in Latvia. The lack of historical knowledge and evolving nature of cyber risks create significant challenges in quantifying and expressing cyber threats in monetary value. Cyber risk modelling is in its infancy, as events and threat vectors are still evolving. Due to the evolving nature of cyber risks, simulating events and fitting into traditional risk management forms are the primary challenges for insurance companies. Despite the increasing relevance of cyber risks to businesses, research on guidelines and methods of mitigating cyber risks with cyber insurance is still limited.

Social implications. Cyber insurance is a direct result of public awareness of cyber threats and preparedness to mitigate business risks. Thus, cyber insurance is an integral part of educating and building a more resilient society.

Originality/Value. The authors propose various approaches to cybersecurity insurance development, such as technology awareness building, standardization of mandatory reporting requirements and public–private partnerships in which the government covers part of the risk to overcome insurability limitations.

Keywords: cyber insurance, cybersecurity, cyber insurance market, cyber risks

INTRODUCTION

With the increasing importance of information technology (IT) in the business and public sectors, there has been a growing impact of cybersecurity threats, i.e., their effect on these sectors' processes. One of the ways to mitigate cybersecurity risks is cybersecurity insurance.

There is no common understanding regarding the essence of cybersecurity insurance. According to Matthew, cybersecurity insurance is an insurance product which is used in protecting businesses as well as individual users from information technology-based risks (Matthew, 2019). Sometimes referred to as cyber liability or cyber risk insurance, its definition has evolved considerably due to new emerging cyber threats. Initially there was a focus on media and software risks, especially banking, and this expanded to network security, unauthorized access, data loss and other virus-related issue coverages (Matthew, 2019). Later cybersecurity insurance also included first-party (relates to loss directly suffered by the insured) and third-party (relates to claims brought by parties external to the contract) coverages, still excluding regulatory claims and fines and penalties (Romanovsky *et al.*, 2019). With the expansion of the Internet of things, cybersecurity insurance includes further contemporary items and issues. Even with the negative worldwide influence of COVID-19 on economic development, the global cybersecurity insurance market forecast is estimated to grow at a CAGR of 21.2% from USD 7.8 billion in 2020 to USD 20.4 billion in 2025 (Research and Markets, 2020).

Latvia as a research object in this relationship between growing IT business, cybersecurity risks and cybersecurity insurance is particularly appealing. Firstly, Latvia is still in the process of integrating into the market economy regarding new services and products that have been around in the Western world for a considerable time. Secondly, information and communication technologies play an important and especially growing role in the Latvian economy – in the last quarter of 2019, this sector shared 5.16% of the whole economy (Central Statistics Bureau, 2020). These results exclude other sectors that are highly dependent on IT: energy, banking, manufacturing, logistics and others. This paper aims to provide an overview of the current situation of cybersecurity insurance, identifying challenges in this recently emerging insurance market in Latvia.

This paper consists of four parts. The authors will start with analysing theoretical literature regarding the costs of cyber threats and cybersecurity insurance. Further on, the research

design and methodology will explain how observance of cybersecurity insurance in Latvia was conducted, and this will be followed by presentation and analysis of the research results. Finally, concluding remarks will close this study.

LITERATURE REVIEW

Cybersecurity insurance is still an evolving subject of research and, therefore, is experiencing harsh debates regarding its definition. Besides the previously mentioned perspective from Matthew, Romanovsky, Ablon, Kuhn and Jones state that "cyber insurance addresses first and third-party losses as a result of a computer-based attack or malfunction of a firm's information technology systems" (Romanovsky *et al.*, 2019). These two definitions show the gaps in comprehension of cybersecurity insurance, for example, what exact risks are included and excluded and whether private customers can attain such insurance coverage. In addition to these researchers (Romanovsky, Anderson, Matthew and others), major contributors to the research field include private think tanks such as FICO and public entities such as governments (the UK is an outstanding example of interconnectivity between insurance brokers and the government) and international organizations (the EU, OECD and others).

Regardless of the definition, an integral part of cybersecurity insurance is estimating the cost of cybercrime – it has to be damaging enough for anyone to be willing to give up part of their income to mitigate the risk. The European Commission's 2007 Communication "Towards a general policy on the fight against cybercrime" has proposed a threefold definition for the cost of cybercrime:

1. Traditional forms of crime such as fraud or forgery, though committed over electronic communication networks and information systems (direct losses)
2. The publication of illegal content over electronic media (cost to society)
3. Crimes unique to electronic networks such as attacks against information systems, denial of service and hacking (defence costs) (OECD, 2017)

Anderson and others have worked on research to investigate the nature and size of the top-ranking cybercrime costs of today, especially since 2012, when the last such report was made (Anderson *et al*., 2019). The following figures give an impression of how valuable the cybercrime industry is and how appealing it makes cybersecurity insurance as a risk effect mitigation tool (see Table 1).

Table 1

Cybercrime types and the value of damage, million, billion £ and USD (2012-2018)

Crime Type	Value of Damage
Online credit card fraud	£731.8 million (UK)
Online bank fraud	£121.4 million (UK)
Authorized push payments	£236 million (UK)
In-person card fraud	£158 million (UK)
Ransomware	Over $10 million (US)
Cryptocrime	$2 billion (US)
Ad fraud	$1-9 billion (US)
Pharmaceuticals	Tens of millions of $ (US)
Coupon fraud	$300m+ (US)
Loyalty-programme fraud	$235 million (US)
Travel fraud	$1 billion (US)
Counterfeit software	$1-9 million (US)
Copyright theft	$10 million (US)
Fake antivirus	$7.1 million (US)
Tech support scams	$39 million (US)
Compromised email	Regulatory and legal costs
Fake companies	Tens of millions of $ (US)
Advance fee fraud	$ 100 million (US)
Business email compromise	$1.3 billion (US)
Telecoms fraud	$7 billion (US)
Wanacry/NotPetya	$1-2 billion (US)
Fiscal fraud	$1-9 billion (US)
Romance scams	$143 million (US)

Source: Anderson *et al*., 2019

Determining cybersecurity crime type and value of damage is only part of implementing cybersecurity insurance as a means to mitigate information technology-related risks. Cybersecurity insurance, just like any other insurance business, has to be economically viable. In order to accomplish this, according to Insurance Europe, certain principles of insurability have to be met: risks must occur randomly, risks must be quantifiable, and a sufficiently large community with assets at risk can be established to share the risk (OECD, 2017). When these criteria are achieved, the creation of an insurance policy can happen – an interaction between demand, supply and cyberspace-related factors.

The OECD points out two factors that have the greatest effect on cybersecurity insurance policy price: first, the difficulty in quantifying a relatively new and evolving risk; second, the potential for significant correlation across insureds, also known as an accumulation risk (OECD, 2017). According to the CRO Forum, quantifiability of cyber risk as a shortfall for the cybersecurity insurance business is mostly due to limited availability of historic data, the changing nature of cyber risk and the lack of transparency about security practices and

past incidents in the corporate world (OECD, 2017). The organization points out that in the case of a cyber risk, there is a huge potential for losses to be correlated across insureds and across various types of coverages provided to a single insured (OECD, 2017). Accumulation risk is therefore due to high levels of interconnectivity – common software vulnerability, information technology service disruptions and critical infrastructure damage.

From potential customers' perspective, according to the OECD, willingness to demand and pay for cybersecurity insurance as a product is most likely affected by a lack of awareness of potential losses from cyber risk, misunderstandings about the need for coverage as well as a potential mismatch between what companies are seeking and the coverage offered – 77% of companies interviewed in the UK in 2016 stated that coverage only partially met their needs, indicating reputational damage and intellectual property theft as the most concerning risks they would like to be covered (OECD, 2017).

Despite the limiting and developing factors of the cybersecurity insurance market, it doubled in the time period between 2015 and 2018, reaching an estimated $4 billion in premiums (Anderson *et al*., 2019). In a similar 2018 report by NetDiligence, the conclusion was that one third of pay-outs are for legal costs such as defence lawyers and settlements; this information has to be considered when calculating total cybersecurity insurance costs (NetDiligence, 2018). An important role in the development of cybersecurity insurance is played by data providers that offer risk assessment to organizations seeking insurance and underwriters, such as *Bitsight*, Security Scorecard and *QuadMetrics* (Anderson *et al*., 2019).

When looking at the Western European market for cybersecurity insurance, the trend is similar. According to a FICO 2017 survey covering 11 countries (from Europe – the UK, Norway, Sweden, Finland and Germany) and 500 companies, the UK leads with 90% of companies having cybersecurity insurance and 37% covering the most likely cybersecurity risks (FICO, 2018). The Nordic countries are not far behind with 76% of Finnish companies, 72% of Norwegian companies and 57% of Swedish companies being cybersecurity insured (FICO, 2018). This survey also reflects Nordic cyberspace's profile – 65% of organizations expected an increase in cyber risks, 41% of organizations experienced an increase in attempted cyber breaches, more than half of organizations were expecting a budget increase for their cybersecurity, 34% of organizations have privacy regulations as the biggest influencing factor in cybersecurity strategy (32% – pressure from customers and investors, 20% – an increase in cyberattacks) and 80% of organizations expect the cybersecurity risk to come from their own ranks, not third-party vendors (FICO, 2018). When analyzing cybersecurity insurance trends across Europe, it is essential to observe the UK. According to a report compiled by the British government in conjunction with Marsh in 2015, the cabinet helped the insurance industry to establish cybersecurity insurance as part of organizations' cybersecurity toolkit by developing a guide on cybersecurity insurance and organizing a data, threat and trend-pooling public forum without revealing anyone's identity (Marsh, 2015). The British example shows that

governmental support is essential in the early developmental stages of cybersecurity insurance.

METHODOLOGY

The main goal of the research is to provide an overview of the current challenges of cybersecurity insurance, focusing on the identification of development constraints and opportunities and the key impact factors of this recently emerging insurance market in Latvia. The research combined qualitative and quantitative methods for exploring and understanding the defined problem statement. In the framework of this research the authors conducted a semi-structured interview with a representative from the Latvian cybersecurity industry and a survey of Latvian insurance companies and Latvian mobile operators in order to understand why cybersecurity insurance is not widely offered on the Latvian market.

Survey of insurance companies

The research team identified 10 principal non-life insurance companies in Latvia: "Balta", "*Baltijas Apdrosinasanas Nams*", "BTA Baltic Insurance Company", "Compensa Vienna Insurance Group ADB Latvian branch", "ERGO Insurance SE Latvian branch", "ADB "Gjensidige" Latvian branch", "If PandC Insurance AS Latvian branch", "Seesam Insurance AS Latvia branch", "Swedbank PandC Insurance AS Latvian branch", and "Balcia Insurance SE". 8 of them are members of the Latvian Insurers Association. The insurance companies were selected according to their expertise at the international level and current exposure in the Latvian insurance market.

Of the ten companies approached, six agreed to the survey, making the response rate 60%. The representatives who answered the questions and shared their experience are managers of various levels or representatives of product development departments, such as Corporate Property Insurance Products Manager; Product Manager; Head of the Commercial Products, Pricing and Risk Underwriting Department; and Head of the Latvian Branch. All companies participating in the survey have already analyzed the inclusion of cybersecurity insurance in their product portfolio.

The authors developed a questionnaire based on the literature review, posing 8 qualitative questions. The survey was conducted in February 2020.

The authors focused on understanding the development of the cybersecurity insurance market. The core research questions were: Has the insurer seen an increase in demand for cybersecurity insurance products from companies in the last 2-3 years? What are the key impact factors influencing the cybersecurity insurance service offer? What are/would

insurance companies consider as contributing factors to the cybersecurity insurance service offer?

Interview with an expert

The research team initiated the research with a face-to-face interview with the Chief Executive Officer (CEO) of Latvian insurance company X, which offers up-to-date high-end insurance solutions, including cybersecurity insurance. At the time of the study, the number of cybersecurity insurance policies issued by Latvian insurers was not large and this segment of the business was just beginning to grow. The expert of company X was selected because this company had issued several cybersecurity insurance policies; accordingly, this was the company with the largest experience of where such risks are located. An interview was conducted in January 2020 in order to find out how long the company had been offering cybersecurity insurance services in Latvia, whether this was popular amongst Latvian entrepreneurs, what restrictions and limitations they were facing and what the company's vision for the future was, including forecasts for the growth in popularity of cyber insurance products. The interview was based on experience and opinion and provides a general idea plus a realistic view of the contemporary expert on current issues regarding cybersecurity insurance from different perspectives: demand, supply, hindrances, and general understanding.

Surveys of Latvian mobile operators

The research team identified all the mobile operator companies operating in Latvia over the last five-year period. The authors sent the questionnaire to the following 3 mobile operators operating in Latvia: "LMT", "BITE Latvija", and "Tele2". At the time of this research, the leader of the Latvian mobile communication market was "LMT" with a 45% market share, followed by "Tele2" with 33% of the market and "BITE Latvija" with a 22% market share according to a Public Utilities Commission report. One representative from each company was selected according to 2 criteria: executive or mid-level management position and direct involvement in the company's cybersecurity management. A response was received from all 3 company representatives, making the response rate 100%.

The mobile communication industry as a possible cybersecurity insurance buyer was chosen because their services largely depend on IT, are widely recognized, have a brand, have a large customer base, hold comprehensive customer data, and have an IT infrastructure critical to their business. All these business conditions make them an appealing target for cyberattacks. Large companies have done a lot to make themselves cyber-secure, yet some risks remain, including through their exposure from third parties,

service providers, product suppliers or customers (Marsh, 2015). But it should be noted that not just business giants are vulnerable to destructive cyberattacks. It is the data, not the size of the company, that makes a business attractive to cyber criminals, especially data such as customer contact information, credit card data, health data, or valuable intellectual property (Armerding, 2015).

The research team developed a questionnaire about cyber insurance based on the literature review. According to Marsh Ltd. research, the potential losses from cybersecurity incidents and cyberattacks fall into the following 11 loss categories: intellectual property theft, business interruption, data and software loss, cyber extortion, cybercrime/cyber fraud, breach of privacy events, network failure liabilities, impact on reputation, physical asset damage, death and bodily injury, and incident investigation and response costs (Marsh, 2015). The questionnaire focuses on malicious attacks because of the much greater damage they can cause compared to non-malicious attacks. The research team approached mobile operators operating in Latvia with questions based on these loss categories as well as questions about their general interest in acquiring a cybersecurity insurance policy.

Asking about different loss categories shows the extent to which cyber risk deserves to be considered and that it is much greater than the current focus on data breaches, which companies these days seem to understand as the biggest threat. This categorization also recognizes that the impact of the attack may be felt well beyond the organization affected. Companies should also consider the impact a cyberattack on a supplier or other third party could have on their own business. In the questionnaire the mobile operator representatives were asked to explain whether they would be interested in insuring their company and which of the loss categories they would most likely be interested in having covered in an insurance policy. The questionnaire focused on cyberattacks and malicious IT failures, since malware and web-based attacks continue to be the most expensive according to Accenture research (Accenture, 2019). The survey was conducted in February 2020.

RESULTS AND DISCUSSION

Results of the interviews with insurance companies

The research results illustrate the immense difficulties and significant challenges in providing cybersecurity insurance. The importance of cybersecurity, at both the corporate and national level, is only growing (Ministry of Defence of the Republic of Latvia, 2019). Cyber risks are not avoidable, but they must be manageable; therefore, the authors emphasize the need to continue working on this topic. The National Cyber Security Index of Latvia is still the lowest in the Baltic states (NCSI, 2019).

The research recommendations and observations aim to highlight the shortcomings of the development of the cybersecurity insurance market, emphasizing that an integrated approach is needed to address them. The authors propose that the principal insurance

companies need to create a structured dialogue to highlight a harmonized framework and the main directions in developing the cybersecurity insurance market. Cooperation between the principal insurance companies would expedite the development of the cybersecurity insurance market, but as this is a competition issue, the possibility of applying such an approach is restricted.

Overall, the outcome of this research of the principal insurance companies provides useful insights on the growth potential, challenges and significant concerns of cybersecurity insurance in Latvia. Respondents of all levels emphasized their main concerns about the current cybersecurity insurance market and highlighted areas for further research and analysis. At the same time, the authors note that there is no clear and harmonized terminology among insurance companies for cybersecurity insurance. Moreover, there are limitations in insurance companies regarding sufficient technically skilled underwriters/brokers to build in-house expertise, which is one of the key findings. One factor that drives the complexity of the underwriting process is that cyber insurance is not a bulk product but is highly tailored to each customer (Franke, 2017).

The key findings from the survey of insurance companies' representatives are shown in Figure 1:

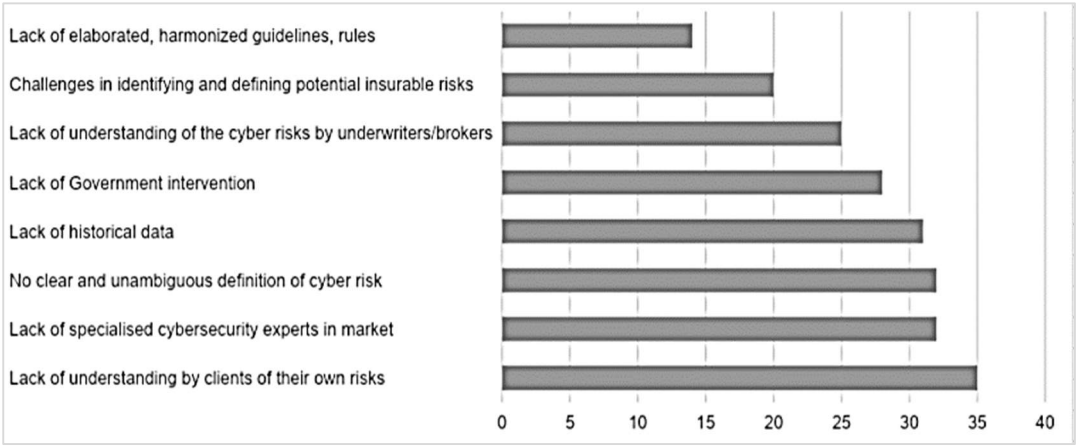

Figure 1 **The sum of representatives' evaluations of the key findings on a scale of 1 to 8 (1 – lower importance, 8 – higher importance)**

Source: survey conducted by the authors

The research highlights a need for an increased awareness of cyber risk on the supply and demand side. Cyber risk is a dynamic risk category that has substantially evolved over time; also, the protective processes and systems are fundamentally evolving (Eling *et al.*, 2019). Lack of understanding by clients of their own risks related to cybersecurity is defined as the main key finding of the survey. Therefore, the key success factor for enhancing cybersecurity insurance development from the authors' point of view is commonly agreed terminology among insurance industry representatives around

cybersecurity insurance key terms. This is also one of the preconditions for establishing common procedures and standards, without which a successfully functioning cybersecurity insurance market is not possible. However, the authors consider that insurance companies need to play a critical role in helping other companies understand potential consequences of cyberattacks and identify insurable cyber risks to increase overall company awareness of cybersecurity, in the form of seminars, educational materials, and conferences.

Cyber risk measurement and management is a challenge for insurance companies (Ruan, 2017). The authors agree that, by nature, a cybersecurity insurance product is a very complex type of insurance, in terms of both indemnification and regulation. Indeed, proper assessment and quantification of an organization's security situation is something that the information security industry has been struggling with for decades and which, to this day, remains elusive (Romanosky *et al.*, 2019). All the respondents share the same opinion that the intangible and pervasive nature of cyber risks and their remodelling into traditional risk management forms and applying appropriate insurance coverage pricing are the primary challenges for insurance companies. The authors consider that international experience of insurance companies must be used to adapt risk management forms already in use. Insurance companies consider business liability coverage for a data breach as the most necessary category of cybersecurity insurance for businesses. At the same time, respondents of all levels were eager to point out that insurance policies could not be standardized but must be custom-based and tailored to the business of a particular company. This means that coverage and terms would vary (Bodin *et al.*, 2018). The authors highlight it as one of cybersecurity insurance's limitations, as custom-based policies require additional time and work from the insurance companies' side.

Very low customer demand, an average of 1-2 applications per year, compared with the possible high cost of risk assessment and valuation from the insurers' side, is not facilitating the cybersecurity insurance offer currently, but at the same time, insurance companies expect a gradual increase in the demand for cybersecurity insurance, mainly driven by increased awareness of risks and by a higher frequency of cyber events. The impact of cybersecurity breaches is often not visible materially, which prevents their impact from being assessed in a sufficiently transparent manner from the outset. The respondents admitted that there is a very high possibility that customers who do not already understand the need for the simplest types of insurance for their business will not be motivated to spend financial resources on a cybersecurity insurance product, speculating that the occurrence of risks defined in the policy is impossible. The authors consider that demand is low due to the fact that insurance can defray only some of the costs of a data breach. As respondents also highlighted in the surveys, even the most comprehensive insurance policies will not ensure full coverage for a business, as provision of cybersecurity requires a strong security culture in companies.

While some insurance companies observe a potential for growth, they still prefer to adopt a careful approach in light of the uncertainties surrounding cyber risk, ranging from difficulties in risk modelling and prediction to adequate cost-effective pricing. There are

many different processes influencing cybersecurity-related decisions inside a company. There are also many different factors, both internal and external, that can influence companies' cybersecurity decision-making and cyber insurance adoption (Labunets *et al.*, 2020). Data and quantitative tools are key obstacles to the development of the cyber insurance industry. Insurers mentioned that lack of data (lack of sufficient amounts of claims data) is an important obstacle to a detailed understanding of fundamental aspects of cyber risk to build adequate models to assure accuracy in risk management. Organizations are wary of releasing too much information about their internal systems to prevent a decrease in reputation as well as leakage of knowledge about weaknesses of the system (Marotta *et al.*, 2017).

From the authors' point of view, effective risk management is essential for success in enhancing cybersecurity insurance development and needs the involvement of the entire insurance industry, associations and the government to maximize data availability.

The authors consider that an important success factor driving cybersecurity insurance is emphasizing the cybersecurity insurance topic and its importance at the governmental level. A strong majority of insurance companies have confirmed that the government should play an important role in fostering good cybersecurity practices by strengthening cybersecurity strategy and in supporting the cybersecurity insurance market through policies and regulation.

From the authors' perspective, if there is no stable supply from the insurance companies' side for cybersecurity insurance products, new players could enter the market such as start-ups, which on the one hand could be potential partners, but on the other could be treated as competitors and might overtake this insurance industry segment.

Expert interview analysis

With the development of modern technology, cyberattacks have become an integral part of the business world, and the fight against these attacks has become a major challenge for many companies. The questions addressed in the interview with the CEO of a Latvian insurance company were as follows: How does one choose an appropriate protection system to help fight against them? Is cyber risk insurance a solution to protect a company from paralysis and cybercrime losses? Do companies in Latvia see a need for cybersecurity insurance, and are insurance companies in Latvia ready for it? In order to objectively assess the influencing factors related to cybersecurity insurance, the expert was mainly asked to speak about challenges and practical experience in implementing this product for more than five years.

The expert clarified that the company does not develop cybersecurity insurance products but finds appropriate solutions for the client. The company has been offering such a service, and he emphasizes that interest is gradually growing. Based on the expert interview it can be concluded that one of the primary caveats for an effective insurance

product is a thorough understanding of the risk faced by policyholders. The biggest interest in cybersecurity insurance products is from the financial sector and companies with large databases, companies whose business depends on technology, and technology service providers. The main impact factors mentioned are the lack of public awareness of the importance of data and the possible consequences of cyberattacks. Simultaneously, the expert highlights that it is important to understand that cybersecurity insurance does not guarantee a reduction in the number of incidents but is only an additional safety pillow. One of the factors promoting the introduction of such a service is the need to educate the public more and talk about cyber protection measures and their need at the national level.

As an impediment, the expert mentions insufficient understanding of cybersecurity insurance and capacity among insurers and the relatively small size of the Latvian market, as well as the lack of real claims and litigation against companies, for example, for stolen data. From the expert's point of view, it will be five to ten years before cybersecurity insurance becomes more popular in Latvia.

Latvian mobile operator survey results

At the start of the questionnaire, all representatives of Latvian mobile operators were asked to rank in order of importance what they consider to be the greatest cybersecurity risks for their company (see Figure 2).

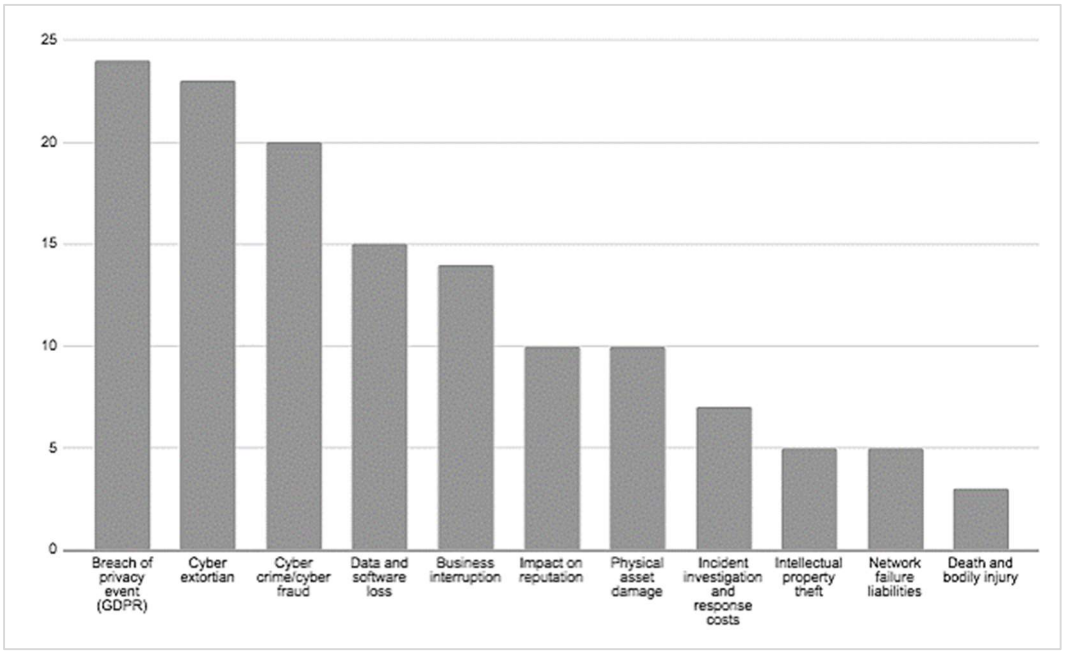

Figure 2 **The sum of representatives' evaluations of the cybersecurity risks on a scale of 1 to 10 (1– lower importance, 10 – higher importance)** Source: survey conducted by the authors

Figure 2 provides insight on the top cyber threats all mobile operator representatives highlighted for their companies. In the framework of the research the authors followed up with questions for the representatives on acquiring cybersecurity insurance for their company. Representatives from 2 mobile operator companies stated that their company doesn't have cybersecurity insurance, but they would be interested to see the possible offers. One representative added that some cyber risks are already covered by their company's general insurance. Representatives whose companies would not be interested in cybersecurity insurance stated that they see cybersecurity insurance as a part of their business continuity plan, not as a separate product. Representatives also mentioned the poor reputation cybersecurity insurance policy cases have gained in the last decade, for instance, the 2011 cyberattacks on Sony involving the theft of personal data such as names, passwords and addresses from more than 100 customers (Independent, 2011). Sony's losses were reportedly estimated to be as high as $2 billion. Despite having cyber liability coverage through the CGL (Commercial General Liability) policy at Zurich American Insurance Company, Sony did not receive compensation for the damages caused by the breach. The CGL policy covered actions taken by Sony, but since the breach was caused by third-party hackers, Zurich American was not obliged to reimburse Sony (Young, 2014). Therefore, the authors consider that in order to establish a better reputation for cybersecurity insurance policies and their liabilities, the Latvian Insurers Association could also play a significant role in promoting cybersecurity insurance by educating businesses about the complexity of policies and their coverage.

In the framework of this survey, of the 2 representatives who would be interested in cybersecurity insurance, only 1 could give an estimate on how much their company would be willing to spend for a cyber policy – estimating it at a price of around 0.005% of the company's yearly turnover. Representatives also suggested that the determining factors for choosing an insurance provider would be insurers' international experience as the most important factor, followed by a customized offer for their business model, and the insurance price as the least important factor.

Representatives who indicated their company's interest in cybersecurity insurance were asked questions about each loss category. Only 1 representative showed interest in insuring risk of intellectual property asset loss due to a cyberattack (expressed in terms of loss of revenue as a result of a reduced market share). For large organizations, intellectual property theft could have the most severe impact. Quantifying the damage caused by the loss of intellectual property or commercially sensitive information is challenging, because such assets are difficult to value, and the loss suffered by an organization depends on how the attacker uses the stolen information. Research conducted by the Oxford Economics team shows that not all industry sectors are attacked in the same way, with industries like defence, chemicals and pharmaceuticals, and creative media being more affected in case of intellectual property theft (Oxford Economics, 2014).

None of the representatives said they would be interested in insuring risk of business interruption, such as lost profits or extra expenses due to unavailability of IT systems. One

representative later stated that such risk is covered under the insurance policy they already have. Also, none of the representatives showed interest in an insurance policy covering costs arising from cyber extortion and cybercrime/cyber fraud, including ransom payment, even if it is evident that representatives recognize it as one of the top cyber risks. But one representative said his company would be interested in insuring loss of revenue due to the impact on reputation after a cyberattack. Reputational damage is a relatively high-frequency event, as most cyber breaches can have a reputational impact if not handled adequately. It is also difficult to quantify damage of this nature, but the research team agrees that such events should be on companies' agendas since proper incident response can limit the severity of loss. Reputational damage accounts for around 5%-20% of the cost of a cybersecurity breach for large businesses. Organizations often overlook certain types of costs of breaches, and so may undervalue their true impact (University of Portsmouth, 2019).

One risk which all representatives indicated as being on their agenda – and 2 representatives stated they would be interested in having covered in cybersecurity insurance – is breach of privacy events, such as fines and penalties related to the European Union's General Data Protection Regulation (GDPR). One representative added that the GDPR has been a top priority for the past 2 years due to its topicality, but it would lose its popularity once everyone gets accustomed to it and more employees get educated in this matter. The research team also agrees that treating the GDPR as the main cybersecurity issue can give a false presumption of organizations' cyber awareness. Applying GDPR standards certainly has a positive effect on many organizations, making them more aware of the information they keep and how they handle it. But having GDPR training won't make any organization more cyberattack-resilient.

In this questionnaire, mobile operator representatives were also asked about their interest in insuring against physical asset damage to their physical property, and only 1 representative stated that they would most likely be interested in covering this risk with insurance. The research team agrees that not all businesses may be affected in the same way in the event of an attack on physical assets, but it should be noted that physical losses are a growing concern because of the interconnectedness of cyberspace and the physical world. An example of a physical loss resulting from a cyberattack is a steel mill in Germany where hackers managed to gain access to the control systems following a successful phishing attack, which targeted individuals for login details. Once access was secured, the hackers were able to cause an unscheduled shutdown of a blast furnace, which resulted in massive damage, according to the German Federal Office for Information Security (Song *et al.*, 2017).

A condensed summary of this questionnaire suggests that 2 out of 3 mobile operators are interested in a cybersecurity insurance policy, but there are only a few risk categories, such as data breaches or the impact on reputation resulting from a cyberattack, that they are interested in insuring. Large companies like mobile operators already have devoted a lot of time and resources to their company's cybersecurity, so they don't see the benefit of

cybersecurity insurance. So the data confirms the authors' observation that businesses in Latvia have low demand for cybersecurity insurance policies because of limited information on how such policies can mitigate cyber risks.

CONCLUSIONS AND DISCUSSION

With a joint analysis of all three sides – the only provider, the potential providers and the possible buyers – important concluding remarks have emerged. According to the research authors and the OECD data, the main challenges in the Latvian market are similar to those in the rest of the OECD countries, and the lack of cybersecurity insurance providers and the low demand from companies to acquire such insurance are a large factor in market growth (OECD, 2017).

There are several reasons for the undeveloped cyber insurance market in Latvia. The lack of historical knowledge and evolving nature of cyber risks create significant challenges in quantifying and expressing cyber threats in monetary value. An important impact factor for the cybersecurity insurance market is the lack of public awareness of cybersecurity risks. There is clearly a need for a more comprehensive understanding of cyber risks, on both the supply and the buyer's side, for the Latvian cybersecurity insurance market to grow further. It is not only about the treatment and assessment of risks, but also understanding businesses' and clients' needs. A set of standards, guidelines and policies could help to clarify what critical business functions should be insured with cybersecurity insurance and how risks interconnect with these functions.

One of the most important factors impacting the cybersecurity insurance market is the small size of the market. Due to the small number of possible purchasers of the product, there is also a trifling number of cybersecurity insurance brokers. The sole provider of cybersecurity insurance in Latvia has chosen to be a mitigator by connecting possible purchasers (those who have already bought the insurance already have high cybersecurity risk awareness) with cybersecurity insurance brokers and experts from abroad rather than hire a permanent office of cybersecurity insurance brokers. As a result, another impact factor of cybersecurity insurance market development is a lack of know-how for cybersecurity insurance in Latvia. Research shows that there is a low demand for cybersecurity insurance policies because of limited information on how cybersecurity insurance policies can mitigate cyber risks.

The research results indicate that the insurance industry is aware of the need for cybersecurity insurance. At the same time, the greatest challenge that all experts and the authors recognize is the need for companies to identify their risks and, first and foremost, perform a risk assessment in order to effectively protect businesses and information in this digital age. Insurance companies can't help to prevent data breaches, but with

cybersecurity insurance they can help in transferring some of the cyber risks instead of the business taking on the risks by itself.

From the authors' point of view, the next stage for cybersecurity insurance development is to include regulatory claims and fines and penalties in the offer, thus making it more attractive and ensuring the demand growth necessary for the economic viability of cybersecurity insurance.

The authors also see the necessity for governmental involvement in developing cybersecurity insurance as of utmost importance. The public sector could pool data related to cyber risks, spread information (CERT.LV is already an existing platform) and create toolkits to inject stimulus for demand and supply of cybersecurity insurance. In the same category of information dissemination, greater media coverage, public education about cyber risks and lobbying from interested parties would also motivate the development of the cybersecurity insurance market in Latvia. Another way of increasing cybersecurity awareness and generating high standards of cybersecurity insurance is to follow the example of the British – introduce and enforce a certification programme (called Cyber Essentials in the UK), which would guide businesses in protecting themselves against cyber threats by setting out the basic technical controls that all organizations should have in place (Marsh, 2015). A common standard certification generated by CERT.LV would put all the companies with cybersecurity risks on the same page regarding requirements, creating a shared understanding of risks and thus cybersecurity insurance.

This research paper offers the beginning of a dialogue between experts, businesses and governance on a general framework and development of the main guidelines for cybersecurity insurance services.

REFERENCES

1. Accenture Security (2019), *Ninth Annual Cost of Cybercrime Study*, available at: https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50 (accessed 2 April 2020).

2. Anderson, R., Barton, C., Bohme, R., Ganan, C., Grasso, T., Levi, M., Moore, T. and Vasek, M. (2019), "Measuring the Changing Cost of Cybercrime", *The 18th Annual Workshop on the Economics of Information Security*, available at https://www.repository.cam.ac.uk/handle/1810/294492 (accessed 29 February 2020).

3. Armerding, T. (2015), "Why criminals pick on small business", *CSO*, 12 January, available at: https://www.csoonline.com/article/2866911/why-criminals-pick-on-small-business.html (accessed 2 April 2020).

4. Bodin, L., Gordon, L. A., Loeb, M. P. and Wang, A. (2018), "Cybersecurity insurance and risk-sharing", *Journal of Accounting and Public Policy*, Vol. 37, No. 6, pp. 527-544.

5. Central Statistics Bureau (2020), *Iekšzemes kopprodukts*, available at: https://www.csb.gov.lv/lv/statistika/statistikas-temas/ekonomika/ikp (accessed 27 March 2020).

6. Eling, M., Wirfs, J. (2019), "What are the actual costs of cyber risk events?", *European Journal of Operational Research*, Vol. 272, No. 3, pp. 1109-1119.

7. FICO (2018), *The Nordics. Views from the C-Suite Survey*, available at: https://www.fico.com/en/latest-thinking/ebook/nordics-views-c-suite-survey-2018 (accessed 16 February 2020).

8. Franke, U. (2017), "The cyber insurance market in Sweden", *Computers and Security*, Vol. 68, pp. 130-144.

9. *The Independent* (2011), "Sony battles to regain trust after data breach", 18 September, available at: https://www.independent.co.uk/life-style/sony-battles-to-regain-trust-after-data-breach-2283560.html (accessed 2 April 2020).

10. Labunets, K., Pieters, W., Eeten, M., Branley-Bell, D., Coventry, L., Briggs, P., Martínez, I. and Sewnandan, J. (2020), *Security Risk Models for Cyber Insurance*, Routledge, Abingdon, pp. 11-26.

11. Marotta, A., Martinelli, F., Nanni, S., Orlando, A. and Yautsiukhin, A. (2017), "Cyber-Insurance Survey", *Computer Science Review*, DOI: 10.1016/j.cosrev.2017.01.001, ISBN: 1574-0137.

12. Marsh (2015), *UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk*, available at: https://www.marsh.com/uk/insights/research/uk-cyber-security-role-of-insurance-in-managing-mitigating-risk.html (accessed 2 February 2020).

13. Matthew, A. (2019), "Cyber Insurance", *International Journal of Engineering and Advanced Technology,* Vol. 8, No. 6, pp. 47-51.

14. NCSI (2019), *National Cyber Security Index,* available at: https://ncsi.ega.ee/country/lv/ (accessed 4 April 2020).

15. NetDiligence (2018), *Cyber Claims Study*, available at: https://netdiligence.com/wp-content/uploads/2018/11/2018-NetDiligence-Claims-Study_Version-1.0.pdf (accessed 17 February 2020).

16. OECD (2017), "Cyber insurance market challenges", *Enhancing the Role of Insurance in Cyber Risk Management,* OECD Publishing, Paris.

17. Oxford Economics (2014), *Cyber-attacks: Effects on UK Companies*, available at: https://www.oxfordeconomics.com/recent-releases/cyber-attacks-effects-on-uk (accessed 2 April 2020).

18. The Public Utilities Commission (2019), *TOP 8: Kas mainijies telekomunikaciju operatoru darbiba un sniegtajos pakalpojumos?*, available at: https://www.sprk.gov.lv/events/top-8-kas-mainijies-telekomunikaciju-operatoru-darbiba-un-sniegtajos-pakalpojumos (accessed 10 April 2020).

19. Research and Markets (2020), *Cyber Insurance Market by Component (Solutions (Analytics and Cybersecurity) and Services), Type (Standalone and Packaged), Coverage (Data Breach and Cyber Liability), Organization Size, End User (Technology and Insurance), and Region – Global Forecast to 2025,* available at https://www.researchandmarkets.com/reports/5178517/cyber-insurance-market-by-component-solutions (accessed 21 February 2020).

20. Romanovsky, S., Ablon, L., Kuehn, A. and Jones, T. (2019), "Content Analysis of cyber insurance policies: how do carriers price cyber risk?", *Journal of Cybersecurity,* Vol. 5, No. 1, pp. 1-19.

21. Ruan, K. (2017), "Introducing cybernomics: A unifying economic framework for measuring cyber risk", *Computers and Security*, Vol. 65, pp. 77-89.

22. Song, H., Glenn, A., Fink, G. A. and Jeschke, S. (2017), "Security and Privacy", in *Cyber-Physical Systems: Foundations, Principles, and Applications*, John Wiley and Sons, Hoboken.

23. University of Portsmouth, Department for Digital, Culture, Media and Sport (2019), *Cyber Security Breaches Survey*, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_d

ata/file/875799/Cyber_Security_Breaches_Survey_2019_-_Main_Report_-_revised.pdf (accessed 2 April 2020).

24. Young, H. (2014), "N.Y. Court: Zurich Not Obligated to Defend Sony Units in Data Breach Litigation", *Insurance Journal*, 17 March, available at: http://www.insurancejournal.com/news/east/2014/03/17/323551.htm (accessed 2 April 2020).