ISSN 2392-1641

Economics and Business Review

Volume 3 (17) Number 2 2017

CONTENTS

ARTICLES

MISCELLANEA

Poznań University of Economics and Business Press

Paper based publication

ISSN 2392-1641

POZNAŃ UNIVERSITY OF ECONOMICS AND BUSINESS PRESS
ul. Powstańców Wielkopolskich 16, 61-895 Poznań, Poland
phone +48 61 854 31 54, +48 61 854 31 55, fax +48 61 854 31 59
www.wydawnictwo-ue.pl, e-mail: wydawnictwo@ue.poznan.pl
postal address: al. Niepodległości 10, 61-875 Poznań, Poland

Printed and bound in Poland by:
Poznań University of Economics and Business Print Shop

Circulation: 215 copies

Economics and Business Review, Vol. 3 (17), No. 2, 2017: 33–50
DOI: 10.18559/ebr.2017.2.3

The cyber-insurance market in Poland and determinants of its development from the insurance broker's perspective[1]

Grzegorz Strupczewski[2]

Abstract: The aim of the paper is to analyze the state of the cyber-insurance market in Poland, and additionally the identification of key determinants of its development, including such issues as cyber-risk perception and the insurability of cyber-risk. Due to the lack of comprehensive, cross-industry insurance data on cyber-insurance, I decided to collect raw data through my own, computer-aided survey amongst insurance brokers operating in Poland. By conducting the survey amongst insurance brokers it was possible not only to collect data describing the state of Polish cyber-insurance market but also to use their expert opinion on various issues relating to cyber-risk. The research presented here is a pioneer in terms of analysis of a cyber-insurance market in a post-communist country such as Poland which is the most important emerging market in the CEE region as well. My paper makes the research perspective broader as most cyber-insurance industry reports have focused ing on the US, the UK or the developed countries of Western Europe.

Keywords: cyber-risk, cyber-insurance, Poland, data breach, risk management.

JEL codes: G22, G32.

Introduction

As mobile technologies advance and cloud computing, corporate bring-your-own-device policies and big data become increasingly popular, cyber-risk has emerged as the major threat for many organizations. At the same time cyber--criminals are using ever more sophisticated tools and state-sponsored espionage is occurring more frequently. The materialization of cyber-risk, under-

[1] Article received 13 October 2016, accepted 15 May 2017. The publication was funded by a grant awarded to the Faculty of Finance of Cracow University of Economics to maintain research potential.

[2] Cracow University of Economics, Faculty of Finance and Law, Department of Risk Management & Insurance, ul. Rakowicka 27, 31-510 Cracow, Poland; grzegorz.strupczewski@uek.krakow.pl.

stood as the failure of information systems or computer crime, led to financial losses in the past year in 16% of enterprises in Poland and 8% of enterprises globally, making it, respectively, the seventh and ninth largest cause of material losses (AON, 2016b).

Cyber-incidents in Europe began to become apparent in 2009 and rose gradually over the next five years, though laws in Europe have less of an emphasis on notification following corporate data breaches and more of a focus on personal control over data held by governments. When cyber-related losses occur in Europe more than half (59 percent) affect personal privacy.[3] A fifth compromise personal financial identity, though this may because fewer data breaches involving consumer payment cards are regularly announced for European organizations. Corporate losses of business income accounted for 12% and corporate loss of digital assets 9% (Ayers, 2015).

Cyber-security is increasingly on the minds of managers as cyber-attacks now regularly cost firms millions in direct and indirect losses due to decreased future revenues and potential legal liability. In the face of more frequent contractual insurance requirements for cyber-liability, forward-thinking companies are taking proactive steps to explore and transfer cyber-risk. Traditional insurance products including property all-risk insurance, general liability insurance and professional indemnity insurance which do not provide full coverage of cyber-risk. New, comprehensive and innovative cyber-insurance is needed to address all aspects of cyber-risk exposure. Demand for cyber-insurance is not equal across the world. The cyber-insurance take-up rate on the North American insurance market is four times that of the European market (42% of organizations purchased cyber-insurance in North America compared to 10% in Europe). The cyber-insurance take-up rate in Poland is unknown but certainly remains very low. The second factor driving companies to purchase cyber-insurance is annual turnover. Most industry reports show a positive correlation between company size and demand for cyber-risk coverage (Advisen, 2016; AON, 2016a). The key drivers for the rapid development of the North American cyber-insurance market are data-breach notification regulations and big losses (data breaches) reported by the media. Europe lacks the strict data-breach regulations that are in place in the US but in April 2016 the European Parliament finally agreed on the *General Data Protection Regulation* (GDPR) which will enter into force in 2018 and is expected to boost the development of the European cyber-insurance market, as occurred in the US.

The aim of this paper is twofold: to analyze the state of the cyber-insurance market in Poland and to identify key barriers to its development,[4] including

[3] Personal privacy includes the loss, exposure, or misuse of an individual's name and address, driver's license, email, birth date, gender, vehicle registration information, photo, fingerprints, credit history, or medical records.

[4] The development is understood as the rise of the cyber-insurance premium.

the perception of cyber-risk and the dilemmas of cyber-risk insurability. Due to the lack of comprehensive, cross-industry insurance data on cyber-insurance I collected raw data using a computer-aided survey amongst insurance brokers operating in Poland. Conducting the survey amongst insurance brokers made it possible to not only collect data describing the state of the Polish cyber-insurance market but also to use their expert opinion on various issues relating to cyber-risk. It is worth mentioning that it became possible to ask more complex questions because insurance brokers are characterized by professionalism and in-depth knowledge of insurance issues. It really added value to the survey.

The research presented here is a pioneering analysis of a cyber-insurance market in a post-communist country such as Poland, which is also the most important emerging market in the CEE region. The paper broadens the research perspective as most cyber-insurance industry reports have focused on the US, the UK or the developed countries of Western Europe. The term cyber-risk can be understood as any risk emerging from the use of information and communication technology that compromises the confidentiality, availability, or integrity of data or services (Eling & Schnell, 2016, p. 12).

The paper consists of 6 sections. The first briefly describes the research sample and structure of the survey questionnaire. This is followed by a presentation of the current state of the cyber-insurance market as the necessary background for further analysis. Section 4 examines key research that has been done on the perception of cyber-risk. Global and local perspectives are taken into consideration. The next section focuses on cyber-risk insurability criteria. I provide a theoretical background and present the results of my survey. The final section identifies key barriers and opportunities for development of the cyber-insurance market and provides final conclusions.

1. Research sample and survey questionnaire

The aim of the survey was to analyze the current state of development of the cyber-insurance market in Poland and the factors determining its development from the insurance brokers' point of view. To this end cooperation was established with the Association of Insurance and Reinsurance Brokers "Polbrokers", which brings together most of the brokers operating on the Polish insurance market.[5] The Association's database of contacts was used and an invitation to participate in the survey was emailed to 627 brokers. To increase the response rate potential respondents were called on the phone and the invitation to complete the survey renewed. Despite these measures a relatively low response rate of 12% was achieved (76 completed questionnaires were collected). This means

[5] According to the Polish Financial Authority there are 1.276 insurance brokers operating in Poland.

that the results of this study cannot be considered representative of Poland's broker environment in its entirety. The sample was too small for statistical purposes. The survey was conducted in May and June 2016. Amongst the respondents 20% were brokers that engaged in the sale of cyber-insurance.

The survey was based on an independently developed questionnaire consisting of seven parts that addressed the following issues:
- the perception of cyber-risk,
- insurance brokers' opinions on cyber-risk insurability,
- what Polish companies know about cyber-insurance,
- the willingness amongst Polish companies to buy cyber-insurance,
- the availability of cyber-insurance to Polish companies,
- the identification of barriers to the development of the cyber-insurance market in Poland,
- a comprehensive description of the activities of insurance brokers who acquire (offer?) and service cyber-insurance.

2. State of the cyber-insurance market

The first dedicated cyber-risk insurance policies appeared at the end of the 1990s in response to Y2K and the attendant problems associated with the turn of the century. For the first time we became aware of the scale of the challenges an economy will face when computer systems go down. The first cyber-policies for insuring property or civil liability offered very limited coverage. Implementing legal coverage of confidential personal data marked the second development stage of cyber-insurance. These policies focused on the costs resulting from uncontrolled breaches of protected information. We are currently in the third stage of development which is characterized by an awareness of cyber-threats, especially outside the US.

According to research done by Advisen (2015) the number of entities purchasing cyber-liability insurance has grown consistently, from barely 35% in 2011 to 61% in 2015, an increase by 26% percentage points. Interest in cyber-insurance has grown quickly primarily amongst large corporations (30% in five years), while growth amongst small companies has increased by a more modest 22%. Research done by Marsh (2015) amongst European companies showed that cyber-insurance is used on a much smaller scale in the old world than in the US. Only 12% of respondents have cyber-insurance, 6% are in the process of concluding insurance agreements, and 27% plan to purchase such insurance in the coming year. Of course this means that a full 55% of respondents see no need to purchase such protection. This should give us cause for thought, especially given that 57% of those without cyber-insurance admit that the main reason they do not have it is that they lack sufficient knowledge about products that could protect them from cyber-threats. This can be taken as a tremendous

challenge for insurance companies and brokers based on the need to reliably educate and inform their clients.

According to estimates done by Allianz (2015) the combined global value of the cyber-insurance market is 2.5 bln USD, of which the US accounts for 90%. However analysts are calling for double-digit growth, which over the coming 10 years, will see this market generate 20 bln USD in premiums. The lion's share of this growth will occur in small and medium-size businesses. Outside the US cyber-insurance is present in Europe (80 mln USD, of which 30 mln USD occurs in Great Britain) and in Japan (70 mln USD), as well as in other highly industrialized countries (Canada and Australia, both 20 mln USD).

Companies that currently purchase cyber-insurance are mainly those in the financial services' sector (22.8%), telecommunications (14.8%), wholesale and retail trade (9.6%) and healthcare (11.7%). However the composition of the types of cyber-risk in the various sectors of the economy can be very different. For example, financial institutions are primarily exposed to leaks of confidential personal and financial data or unauthorized system access, which may result in a loss of reputation and business interruptions. Companies in high-tech sectors, such as pharmaceutical companies, are much more vulnerable to intellectual property theft. Industrial plant, manufacturers and media providers should pay particular attention to protecting electronic (particularly remote) systems for controlling machines and devices.

Cyber-insurance programmes make it possible to cover the effects of a variety of events and unforeseen expenses. When choosing a particular type of insurance protection the potential internal threats that the organization faces should first be analyzed, as should the structure of the damages occurring on the market. As the data shows cyber-risk in enterprise most often results in the company losing its reputation (61%), experiencing a break in operations (49%) and having to pay damages due to breaches in personal data protection (45%) (Allianz, 2015).

According to various forecasts cyber-insurance in the short and medium term is set to undergo dynamic changes, which may be characterized as follows (Allianz, 2015):

1. Gradually limiting the range of cyber-risk coverage in traditional policies with a simultaneous increase in the availability of specialized cyber-insurance, particularly in civil liability insurance.
2. To verify the adequacy of insurance coverage in the face of personal injury claims and claims for damages.
3. The growing penetration of cyber-insurance will allow insurers to group clients and offer products that better meet the specific needs of various entities.
4. Increased awareness about insurance in the business world and, at the same time, greater familiarity with cyber-risks amongst insurance companies.
5. Improved methods of reacting to crises caused by data breaches, which should rein in the extent of damages.

The survey I conducted amongst insurance brokers operating in Poland showed that only 20% offer insurance contracts that protect against cyber-risks. 71% attribute the low share to a lack of interest on the part of clients, while 12% admit to lacking knowledge themselves about cyber-insurance. This differs from the catalogue of reasons for not using cyber-insurance given by companies in Western Europe and the US where there is a preference for investing in technical IT security solutions over purchasing insurance, a lack of appropriate products offered on the insurance market, a lack of education on the subject amongst brokers, a failure to understand the benefits of cyber-insurance, a fear that cyber-insurance is excessively costly or that it is excessively complicated and a lack of acceptance of the excessive franchise costs and one's own costs (Glascott & Aisen, 2013).

From amongst Polish brokers actively offering cyber-insurance 47% write premiums that do not exceed 10.000 USD annually, while 13% take in premiums that exceed 15.000 USD. Unfortunately a third of the respondents opted not to answer this question. Healthcare, financial services and the IT sector show equally the highest demand for cyber-insurance (each accounted for 15% of the total, or a combined 45% of enterprises with cyber-insurance). Trading companies and public sector entities are also often listed amongst buyers of cyber-insurance (12% each). 67% of the cyber-insurance agreements concluded on the Polish market are stand-alone policies, meaning specialized insurance products dedicated exclusively to cyber-risks. In other cases brokers use additional clauses to extend the coverage afforded by standard property insurance.

The most frequently chosen scope of insurance coverage is the area of civil liability for the breach of privacy of a third person (24%). Enterprises also often opt to insure against loss resulting from the loss of or damage to electronic data (14%) or the result of interrupted operations following IT outages. A number of brokers state that clients which they represent purchase insurance protection against cyber-extortion, though information about such policies is treated as confidential. The structure of sales on the global market is quite similar: The five most frequently insured risks include breach of privacy, data and software loss, incident response costs, cyber-extortion and business interruptions (RMS, 2016).

In seeking an effective means of interesting enterprises in purchasing cyber-insurance most brokers agree that experience with damage has the largest influence on the decision to purchase a policy (54% of respondents indicated as such). That loss experience leads to a real awareness of threats. Respondents further indicated that, in addition to those threats, media coverage of the spectacular cyber-damages occurring in the world poses an equally strong incentive to purchase insurance. Other reasons given include the prompting of brokers (27%) and company risk management policy (13%).

According to information provided by brokers the amount of damages incurred by those with cyber-insurance is still small. Over the past five years

a total of 17 claims have been noted for an average of 3.4 per year. This would seem to justify the conclusion that, on the Polish market, cyber-insurance is a no-claim product. However one may expect, following the American market's lead, that claims on this type of insurance will rise with the coming into force of the EU *General Data Protection Regulation* and the greater dissemination of cyber-policies.

3. Cyber-risk perception — a global perspective

As the results of AON's research[6] show (AON, 2016b), a comparison of the assessment of particular types of threats on a global and local scale did not reveal a clear difference in the perception of cyber-risk. In both cases the risk is amongst the top ten most serious issues that organizations face (it is the ninth most serious, to be exact). Furthermore the decision to take up cyber-insurance corresponds with the currently low perception amongst Polish companies of the risk of electronic crime being committed. However holders of such insurance are, in large measure, satisfied equally with the general terms and conditions and the coverage limits on their insurance. In comparison with the results of global research the share of insurance is more than half lower and is generated practically exclusively by the needs of financial institutions. It is also worth mentioning that the geographical distribution in the framework of the global research is not homogeneous: The highest penetration may be found in the US where 42% of respondents indicated they had purchased insurance. Companies in South America, Africa and the Middle East, on the other hand, are even less insured than their Polish counterparts (7%).

Despite the almost daily publication of information about new cyber-breaches only 34% of organizations that responded to the SANS survey have cyber-insurance, with another 12% reporting that they are self-insured. Unfortunately only 60% of this population indicated that they actually understand the characteristics and limits of their insurance coverage (SANS, 2016). The importance of cyber-risk has clearly increased over the past five years. In 2015 29% of respondents indicated that cyber-risk is an extremely serious issue for organizations. That is up from the 20% reported in 2014 and 16% in 2011 (Figure 1). At the same time the percentage of people who considered the problem trivial (mild and very mild) fell to 7% over the same period (Advisen, 2015).

[6] The global edition of the survey includes responses from 1.418 representatives of companies and institutions, who in their professional practice deal with issues of risk management and insurance. Enterprises participating in the study represent more than 30 different industries and conduct operations in 60 countries. The Polish edition of the survey collected responses from 168 company representatives.

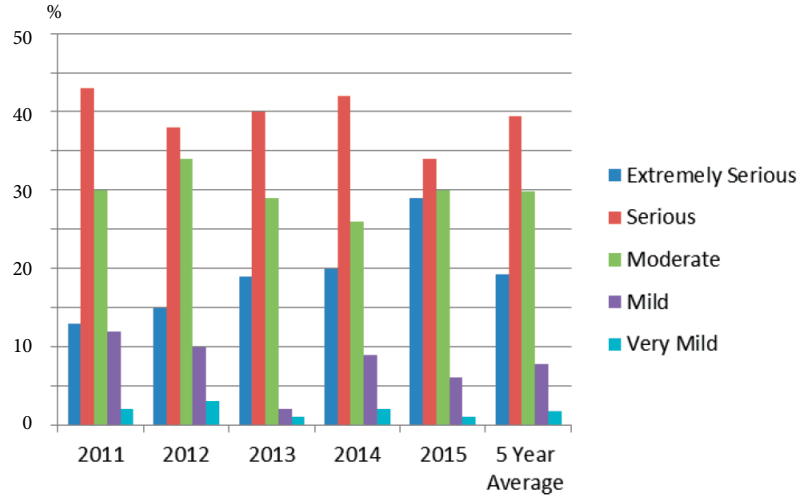

Figure 1. How would you rate the potential dangers posed to your organization by cyber-& information security risks?
Source: Advisen (2015)

An essential factor conditioning the perception of cyber-risk is company size. The larger the company, the more seriously it views this risk. A comparison of the reactions of small firms with an annual turnover below 250 mln USD and large enterprises with revenue exceeding 10 bln USD (Figure 2) led to these conclusions about firm size and risk perception. Over the five-year period an average of 14.4% more large corporations saw cyber-risk as at least a moderate risk, than their smaller counterparts.

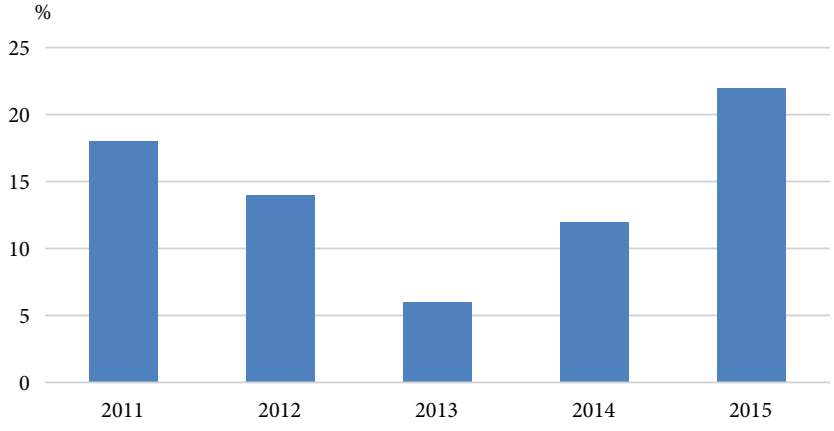

Figure 2. Differences between respondents from small businesses and the largest enterprises saying that cyber-risk poses at least moderate risk for their organizations
Source: Author's own work based on Advisen (2011–2015)

In annual research conducted by Advisen,[7] risk managers and board members were asked to assess the scale of the threats resulting from particular types of cyber-risk from the perspective of their organization. A scale of 1 to 5 was used, with 1 being the minimum degree of threat. The results of regularly con-

Table 1. Average weighted grades of cyber-risk types in years 2011–2015

Type of cyber--risk	2011	2012	2013	2014	2015	Average grade	Change 2011/ 2015 (%)
1	3.56	3.71	3.71	3.73	3.82	3.71	7.3
2	2.82	2.65	2.80	2.89	2.96	2.82	4.9
3	3.28	3.14	3.16	3.33	3.44	3.27	4.9
4	3.28	3.42	3.28	3.37	3.55	3.38	8.2
5	n/d	n/d	3.44	3.60	3.79	3.61	10.2
6	n/d	3.40	3.41	3.50	3.48	3.45	2.4
7	3.58	3.68	3.69	3.80	3.77	3.70	5.3
8	2.97	3.01	3.02	3.04	3.09	3.03	4.0
9	3.29	2.96	2.94	3.06	3.11	3.07	–5.5
10	3.29	2.88	2.91	3.09	3.16	3.07	–3.9
11	n/d	3.50	3.58	3.66	3.79	3.63	8.3
12	3.38	3.34	n/d	3.60	3.60	3.48	6.5
13	n/d	n/d	3.15	3.34	3.41	3.30	8.3

Description:
1 – privacy violation/data breach of customer privacy
2 – theft or loss of customer intellectual property
3 – theft/loss of your organization's assets (including intellectual property)
4 – denial of service attack against your network or virus
5 – malware in your network
6 – damage to your organization's reputation in relation to social media
7 – damage to your organization's reputation as result of data breach
8 – employment practices' risk due to use of social media
9 – business interruption due to disruption in the customer's network
10 – business interruption due to disruption in the supplier's network
11 – incurring costs and expenses from a cyber-attack
12 – business interruption due to disruption in your organization's network
13 – cyber-attacks related to the introduction of your device policy in your organization

Source: Author's own work based on Advisen (2011–2015).

[7] This is an annual survey of cyber-risk management practices in European enterprises carried out in collaboration with Zurich. The respondents are executives, risk managers and other individuals dealing with risk management in enterprises and institutions. Large European companies with turnover exceeding 1 bln GBP predominate in the research.

ducted research are published in an annual report. On the basis of the reports on research carried out in 2011–2015 I synthesized partial results and undertook an analysis of the changes in the perception of cyber-risk over the five-year period. Weighted averages were calculated for the different types of cyber-risk in subsequent years, the arithmetic mean of the assessment during the 5-year period and also the percentage change in the assessment of each risk that occurred between 2011 and 2015 (Table 1).

Two types of risk were perceived to pose the highest threat: breach of clients' personal data and the loss of company reputation as a consequence of data breaches. These were ranked the highest both for the individual years of the survey and as an average across the period. The danger of infecting one's network with malware and the need to invest in fighting cyber-attacks were indicated as two other very important cyber-risks (average assessment of 3.63 and 3.61, respectively). These risks were also seen to be growing the fastest (10.2% and 8.3%, respectively). It is worth noting that there is little variation in the assessments between individual risks (variability 8.51%), which may attest to the difficulty respondents have in recognizing the different aspects of cyber-risk at a high level of detail.

European corporate boards and risk managers (CROs – Chief Risk Officers) largely recognize threats arising from cyber-risk more than their counterparts in the US. 54% of European managers, but barely 45% of Americans, believe cyber-risk constitutes a serious problem for organizations. From amongst CROs the percentages are 69 and 58, respectively, so the difference with regard to cyber-risk is even larger (Advisen, 2011).

Finally, some discrepancies were identified between the list of cyber-risks considered to be the most serious and those which are in fact responsible for the greatest losses. Risks to which data are exposed, computer programs and databases, as well as employees and contractors are mentioned as key threats, while the most frequent materialization of cyber-risks are in fact employees and contractors, electronic data resources and mobile devices (SANS, 2016).

4. Cyber-risk perception – the Polish perspective

In the opinion of the brokers surveyed the majority of Polish entrepreneurs (59%) do not understand the essence of cyber-threats. Only every fourth entrepreneur (26%) has an appropriate awareness of the risk. Regardless of the degree of recognition of cyber-risks it may cause certain attitudes amongst entities affected by the risk. 65% of the respondents believed entrepreneurs did not perceive cyber-risk as a serious threat to their business. According to only 13% of brokers managers of companies appreciate the importance of cyber-crime. It can be assumed that the low interest amongst companies in buying cyber-insurance has an overwhelming influence on the formation of brokers' opinions.

The low level of risk perception directly limits interest in buying cyber-security. Studies show that 76% of respondents agree with this statement and only 8% do not. While an equally high percentage of respondents were critical of the level of knowledge that Polish entrepreneurs possess about cyber-insurance (62%), brokers did appreciate changes clients have adopted over the past three years. 47% of respondents believe that the level of enterprise knowledge about cyber-insurance improved and only 15% fail to see any positive changes. When it comes to changing interest in purchasing cyber-insurance policies brokers are more divided. Every third respondent (34%) noted an increase in demand though 30% of brokers failed to see any change. It is worth noting that brokers' predictions for the near future are optimistic: The vast majority predict that enterprise knowledge about cyber-insurance will rise (78%), and that increased interest in buying cyber-insurance (65%) will follow.

5. The insurability of cyber-risk

A fundamental issue for cyber-insurance is the question of the insurability of cyber-risk being fulfilled by the cyber-risk criteria formulated by Berliner (1982). In his famous work „the limits of the insurability of risks", Berliner elaborated nine conditions: randomness (of the loss occurrence), maximum possible loss, average loss amount upon occurrence, average period of time between two loss occurrences, insurance premiums, moral hazard, public policy, legal restrictions and cover limits.

Eling and Wirfs (2016) discuss the limits of insurability in their research and put forward the following conclusions:

- The positive influence of the law of large numbers on the distributing risk in cyber-risk portfolios built by insurance companies is limited due to the small number of persons insured.
- The lack of historical data, combined with uncertainty regarding the choice of an appropriate model of random variable distribution, force insurance companies to charge a premium higher security overhead and this in turn reduces the attractiveness of cyber-security for customers and drives their cost to a prohibitive level.
- The dynamic character of cyber-risk may render historical data on damages inadequate for forecasting.
- A given entity's level of cyber-risk may depend strongly on the IT safety standards adopted by another company with whom it cooperates but whose computers may become a „back door" for malware. The result of such contingencies is the lack of full control over the risk level covered by the insurance. Computer security organization depends not only on preventive actions but also the effectiveness of security systems in the entities cooperating with it. A global computer network is a system of connected serv-

ers with a level of security in which the weakest link has the largest impact. There are insufficient economic incentives to invest in reducing cyber-risk, but doing so is a common condition of insurance coverage.
– A high likelihood of catastrophic events that are difficult to assess.
– Distribution of losses caused by cyber-risks can be „short-tailed" or „long-tailed" in shape. The latter will occur in the context of events such as a DDoS attack, which immediately paralyzes the system's organization, but the consequences of the incident are properly resolved within a few hours. Long-tail claims, on the other hand, are characterized by sneaking spyware (malware) into a system, which can then remain undetected for many months and generate financial losses that will be spread out over a considerable amount of time. A similar time schedule will have a third party claim brought under the responsibility of the data controller for breach of the security of personal data and will follow a similar time schedule.
– Cyber-risks can have negative consequences both for the insured person (first-party losses), as well as for third parties (third-party losses) which is associated with some difficulties at the stage of building the range and defining the subject of the insurance.
– The correlation between the cyber-damages that may result from a single cause is another extremely difficult issue. It is highly probable that cyber-risk does not meet the requirement of event independence.

Other publications added also the asymmetry of information which can translate for insurance companies into the risk of negative selection and morale hazard (Gordon, Loeb, & Sohail, 2003).

Mindful of the above dilemmas facing the insurability of cyber-risk insurance company underwriters exercise extreme caution in taking on such risk. That caution finds expression in the long list of reasons that applications for cyber-insurance are rejected, the most common of which include: objections to IT security control procedures, a failure to keep security systems up to date, a lack of crisis planning, and unacceptable practices for the creation and archiving of storage backups (Sigma, 2017).

The problematic insurability of cyber-risk is observed not only in scientific publications and industry reports but also by insurance brokers. Respondents were asked to assess eight factors of risk insurability (here a 1–5 scale was used, with 1 being a minimal problem and 5 a very serious one). Then, on the basis of the responses, the weighted average rating for each factor was determined and the most important challenges facing the insurance industry were ranked in the context of the possibility of offering cyber-insurance (Table 2).

According to the respondents the biggest practical problems are associated with the scarcity of historical data about damages, making it impossible to precisely estimate the average loss from a single event (3.53). Few attributed lower weight to the limited possibilities of influence on the amount of maximum loss (3.39) – for example, through preventive measures or safety procedures, though

Table 2. Factors of cyber-risk insurability

Factors of risk insurability	Weighted grade
Average loss per occurrence	3.53
Maximum possible loss	3.39
Asymmetry of information	3.33
Lack of risk-adjusted premium	3.28
Limits of coverage	3.25
Prevalence of risk	3.17
Legal environment	2.95
Randomness of loss occurence	2.84

Source: Based on own study.

practice shows that these do not significantly reduce risk exposure. The complexity of security information systems, the interconnectedness of entities through the Internet, and above all, a high degree of dependence on the risk level of the individual behaviour of individuals make the problem of asymmetric information – widespread in the insurance industry – of particular importance in the context of cyber-security. This was also noted by brokers, who ranked it high (3.33). With the current state of the market, and given the paucity of historical data about damages, it is not possible to quote premiums adequate to the level of risk brought by individual policyholders (3.28). Underwriting has been fairly superficial with a small number of criteria taken into account when premiums are differentiated. Another problem preventing the market from functioning normally is the available limits of insurance coverage being kept low, combined with relatively high deductibles. This practice flies in the face of the classical principle of having full insurance protection. These problems stem indirectly from another problem that the respondents raised – the insufficient dissemination of cyber-security at the current stage of market development. It seems, however, that this situation will soon normalize as the significant increase in demand for cyber-security occurs which is called for in forecasts.

6. Barriers and opportunities to development of the cyber-insurance market in Poland

Considering global tendencies in the evolution of cyber-insurance, various underwriting issues and the realities of the European market, the following hypotheses about the catalysts of and barriers to the development of cyber-insurance in Poland are described. The catalysts include:

- loss ratio (the presence of large damage caused by large-scale attacks by hackers, publicized in the media);
- regulations (adoption and entry into force of the *General Regulation on Data Protection* provides for heavy fines for the infringement of the security of personal data);
- social attitudes (increased privacy needs as a response to the growing presence of IT technology in everyday life);
- competition in the cyber-insurance market (the introduction of cyber-insurance policies offered by an increasing number of insurance companies will bring about pressure marketing and awaken the need to purchase insurance protection against cyber-threats);
- imitation effect (it is expected that once a certain critical mass in the number of entities purchasing cyber-insurance is attained a, further increase in sales will be much easier).

Though the potential for the cyber-insurance market to develop in Europe and Poland appears to be tremendous, a few major barriers, centred mainly around underwriting, do exist. They include:

- insuring cyber-risk is problematic (the interdependence of damages, asymmetric information, negative selection);
- the paucity of historical data about damages makes it difficult to assess risk precisely;
- risk control is ineffective (high IT security standards amongst the insured does not guarantee that risk levels will be reduced because the co-operating companies and other third parties with direct access to the IT system of the insured may, through "the back door", become a source of infection);
- awareness of cyber-threats is not always reflected in the decision to purchase insurance protection;
- a preference for investing in IT equipment and software instead of purchasing insurance;
- a failure to understand cyber-insurance (a popular misconception amongst management is that traditional insurance products provide sufficient protection against cyber-risk);
- the dynamic nature of cyber-risk (the rapidly changing nature, source and intensity of cyber-threats hinders the construction of insurance products and risk assessment).

As a professional group insurance brokers maintain regular contact both with insurance companies and insurance buyers (companies and institutions), and thus are well positioned to assess the mechanisms of the market in which they operate. To verify the above hypotheses, study participants were asked to identify the most significant barriers to the development of the cyber-insurance market in Poland. The following issues influencing supply and demand factors were identified.

The demand barriers (their source and possible changes rest with clients):
- unforeseen or underestimated threat of cyber-risk (29.7%);
- a lack of media information about cyber-damages or a lack of cyber-damages to one's personal property (12.9%);
- entrepreneurs unaware that cyber-risk is insurable (9%).

Supply barriers (their source and possible changes rest with insurers):
- cyber-insurance is too expensive (11.6%);
- insufficient promotion of cyber-insurance by insurance companies (9.7%);
- insufficient availability of cyber-insurance and a failure to adjust it to clients' needs (9.7%);
- insufficient competency on the part of brokers with regard to cyber-insurance due to a lack of training on available products offered by insurance companies (4.5%).

The remaining barriers (their source cannot be clearly attributed):
- cyber-insurance is highly complicated (6.5%);[8]
- other.

Conclusions

In this paper factors determining the development of the Polish cyber-insurance market have been analyzed. Stimulants of and barriers to the development have been indicated based on the results of a survey and reports from entities (insurance brokers) operating in the insurance industry. Particular focus was placed on the perception of cyber-risk as a key determinant of demand and the insurability of cyber-risk as a key determinant of supply. Spreading cyber-risk encourages enterprise, governments, the justice system, specialists and consumers to look further at the nature of the risk and its possible consequences. Awareness of the need to have cyber-insurance is growing slowly; however, from the point of view of insurance companies, designing and underwriting this product has proven far from simple.

Our survey showed that in Poland only every fifth broker offers cyber-insurance.[9] Such a modest share is largely the result of limited interest on the part of enterprises in purchasing cyber-policies and the insufficient preparation of brokers to set up this insurance. Companies that already carry cyber-insurance tend to be in healthcare, financial services and the IT industries. From amongst the wide range of insurable events, the greatest needs include risks such as breach of privacy, data and software loss and business interrup-

[8] There is no evidence upon which to determine whether the insurance is in fact highly complex or merely seen as such by enterprise.

[9] It's worth remembering that due to the low response rate, the results of the survey are not representative.

tion. Incentives compelling enterprises to purchase cyber-insurance include experiencing cyber-damage to one's own property, the media spreading information about large-scale cyber-damage and the prompting of brokers.

A significant difference was noted in the perception of cyber-risk as a threat to organizations by enterprises in Poland, Western Europe and the United States. While in highly developed countries roughly half of company boards were aware of cyber-threats, in Poland – according to brokers – the share is much smaller. Respondents believed that demand for cyber-insurance in Poland may not keep pace with the anticipated growth in the awareness of threats. An important supply barrier this market faces is the remarkably cautious approach insurers are taking. While low level market saturation and the high probability of growth should encourage insurers to develop the cyber-insurance they offer the Polish and European markets diverge considerably. This is due to the fundamental objections insurance companies have to particular aspects of cyber-risk.

Practitioners on the insurance market, using the achievements of academics, pointed out what they believe are the most important barriers to cyber-risk being fully insurable. These include a serious lack of historical data about existing damage, an inability to model maximum probable loss, an inability to perform precise, individual underwriting and a high degree of information asymmetry. Other technical problems stem from the cumulative risk of loss or difficulty in defining the object of insurance and risk exposure (the possible sphere of perpetrators and targets of cyber-attacks and the assessment of the value of the subjects to be insured).

Cyber-threats not only stimulate demand for cyber-insurance but also have a wider influence – they demonstrate the validity of implementing a risk management policy in enterprises and strengthen its role (AON, 2016b). Appropriate information risk management strategies, and especially controlling for this risk, can, according to experts, reduce the risk of cyber-attacks by 80% (Allianz, 2015). This means that a certain residual risk continues to exist which can be financed through the purchase of cyber-insurance. Delivering advanced cyber-risk solutions without a doubt will become one of the most important tasks the insurance industry will face, not only in Poland, but throughout the world.

In summary, the strong incentives to purchase cyber-insurance (mainly the growing risk of cyber-threats) are tempered by equally strong growth barriers, the source of which must be sought on both the supply and demand sides of the equation. One may expect that, in the medium term, the supply barriers will be eliminated (by insurance companies and other entities operating on the insurance market) while in the long term, this market's growth will be dictated by demand factors.

References

Advisen. (2011, March). Information security and cyber liability risk management. Retrieved April 12, 2016, from http://www.advisenltd.com/wp-content/uploads/Cyber_Risk_Management_Survey_Report.pdf

Advisen. (2012, October). Information security and cyber liability risk management. Retrieved April 12, 2016, from http://www.advisenltd.com/wp-content/uploads/Zurich_2012Cyber_SurveyReport.pdf

Advisen. (2013, October). Information security and cyber liability risk management. Retrieved April 12, 2016, from http://www.advisenltd.com/wp-content/uploads/information-security-cyber-liability-riskmanagement- zurich-2013-10-18.pdf

Advisen. (2014, October). Information security and cyber liability risk management. Retrieved April 12, 2016, from http://www.advisenltd.com/wp-content/uploads/information-security-cyber-liability-riskmanagement- white-paper-10-28-2014.pdf

Advisen. (2015, October). Information security and cyber liability risk management. Retrieved April 12, 2016, from http://www.advisenltd.com/wp-content/uploads/2015/10/information-security-cyber-liability-risk-management-report-2015-10-16.pdf

Advisen. (2016, October). 2016 Survey of cyber insurance market trends. Retrieved April 17, 2017, from http://www.advisenltd.com/2016/10/25/2016-survey-cyber-insurance-market-trends/

Allianz. (2015). A guide to cyber risk. Managing the impact of increasing interconnectivity. Retrieved November 12, 2015, from www.agcs.allianz.com

AON. (2016a). Cyber-the fast moving target. Retrieved April 17, 2017, from http://www.aon.com/attachments/risk-services/cyber/2016-Captive-Cyber-Survey-Interactive.pdf

AON. (2016b). Zarządzanie ryzykiem i ubezpieczeniami w firmach w Polsce. Report AON Poland 4th edition. Retrieved July 12, 2016, from http://insight.aon.com/PL_2016ARSNEWS_DownloadAonPL

Ayers, E. (2015, October 8). Advisen Loss Insight: Europe's cyber and privacy landscape. *Cyber Risk Network*. Retrieved July 20, 2016, from http://www.cyberrisknetwork.com/2015/10/08/advisen-loss-insight-europes-cyber-and-privacy-landscape/

Berliner, B. (1982). *Limits of insurability of risks*. Englewood Cliffs, NJ: Prentice-Hall.

Eling, M., & Schnell, W. (2016, November). Ten key questions on cyber risk and cyber risk insurance. *The Geneva Association*. Retrieved April 18, 2017, from https://www.genevaassociation.org/media/954708/cyber-risk-10-key-questions.pdf

Eling, M., & Wirfs, J. H. (2016). Cyber risk: Too big to insure?. *University of St. Gallen*. Retrieved April 15, 2016, from http://www.ivw.unisg.ch/~/media/internet/content/dateien/instituteundcenters/ivw/studien/cyberrisk 2016.pdf

Glascott, M. T., & Aisen, A. J. (2013). The emperor's new clothes and cyber insurance. *Federation of Defense & Corporate Counsel Quarterly*, *Spring 2013*, 200-225. Retrieved May 3, 2016, from http://www.thefederation.org/documents/22.The%20Emperors%20New%20Clothes.pdf

Gordon, L. A., Loeb, M. P., & Sohail, T. (2003). A framework for using insurance for cyber-risk management. *Communications of the ACM,* 44(9), 70-75.

Marsh. (2015, October). European 2015 cyber risk survey report. Retrieved April 11, 2016, from http://uk.marsh.com/Portals/18/Documents/European%202015%20Cyber%20Risk%20Survey%20Report-10-2015.pdf

RMS. (2016, February). Managing cyber insurance accumulation risk. *Risk Management Solutions, Cambridge Centre for Risk Studies*. Retrieved May 12, 2015, from www.cambridgeriskframework.com/getdocument/39

SANS. (2016, June). Bridging the Insurance/InfoSec Gap: The SANS 2016 Cyber Insurance Survey. Retrieved July 1, 2016, from https://www.sans.org/reading-room/whitepapers/legal/bridging-insurance-infosec-gap-2016-cyber-insurance-survey-37062

Sigma. (2017). Cyber: getting to grips with a complex risk. *Sigma*, 1/2017, *SwissRe Institute*. Retrieved April 18, 2017, from http://www.swissre.com/library/sigma_01_2017_en.html

Aims and Scope

Economics and Business Review is the successor to the Poznań University of Economics Review which was published by the Poznań University of Economics and Business Press in 2001–2014. The Economics and Business Review is a quarterly journal focusing on theoretical and applied research work in the fields of economics, management and finance. The Review welcomes the submission of articles for publication dealing with micro, mezzo and macro issues. All texts are double-blind assessed by independent reviewers prior to acceptance.

The manuscript

1. Articles submitted for publication in the **Economics and Business Review** should contain original, unpublished work not submitted for publication elsewhere.
2. Manuscripts intended for publication should be written in English, edited in Word in accordance with the **APA editorial** guidelines and sent to: secretary@ebr.edu.pl**.** Authors should upload two versions of their manuscript. One should be a complete text, while in the second all document information identifying the author(s) should be removed from papers to allow them to be sent to anonymous referees.
3. Manuscripts are to be typewritten in **12' font in A4 paper** format, one and half spaced and be aligned. Pages should be numbered. Maximum size of the paper should be up to 20 pages.
4. Papers should have an abstract of not more than 100 words, keywords and the Journal of Economic Literature classification code (**JEL Codes**).
5. Authors should clearly declare the aim(s) of the paper. Papers should be divided into numbered (in Arabic numerals) sections.
6. **Acknowledgements** and references to grants, affiliations, postal and e-mail addresses, etc. should appear as a separate footnote to the author's name a, b, etc and should not be included in the main list of footnotes.
7. **Footnotes** should be listed consecutively throughout the text in Arabic numerals. Cross-references should refer to particular section numbers: e.g.: See Section 1.4.
8. **Quoted texts** of more than 40 words should be separated from the main body by a four-spaced indentation of the margin as a block.
9. **References** The EBR 2017 editorial style is based on the **6th editio**n of the Publication Manual of the American Psychological Association (**APA**). For more information see APA Style used in EBR guidelines.
10. **Copyrights** will be established in the name of the **E&BR publisher**, namely the Poznań University of Economics and Business Press.

More information and advice on the suitability and formats of manuscripts can be obtained from:

Economics and Business Review
al. Niepodległości 10
61-875 Poznań
Poland
e-mail: secretary@ebr.edu.pl
www.ebr.ue.poznan.pl

Subscription

Economics and Business Review (E&BR) is published quarterly and is the successor to the Poznań University of Economics Review. The E&BR is published by the Poznań University of Economics and Business Press.

Economics and Business Review is indexed and distributed in ProQuest, EBSCO, CEJSH, BazEcon and Index Copernicus.

Subscription rates for the print version of the E&BR: institutions: 1 year – €50.00; individuals: 1 year – €25.00. Single copies: institutions – €15.00; individuals – €10.00. The E&BR on-line edition is free of charge.

Correspondence with regard to subscriptions should be addressed to: Księgarnia Uniwersytetu Ekonomicznego w Poznaniu, ul. Powstańców Wielkopolskich 16, 61-895 Poznań, Poland, fax: +48 61 8543147; e-mail: info@ksiegarnia-ue.pl.

Payments for subscriptions or single copies should be made in Euros to Księgarnia Uniwersytetu Ekonomicznego w Poznaniu by bank transfer to account No.: 96 1090 1476 0000 0000 4703 1245.