BIGS | Policy Paper

Brandenburg Institute for SOCIETY and SECURITY

BIGS
BRANDENBURGISCHES INSTITUT
für GESELLSCHAFT und SICHERHEIT

Cyber Insurance as a Contribution to IT Risk Management

An Analysis of the Market for Cyber Insurance in Germany

Baban, Gruchmann, Paun, Peters, Stuchtey

BIGS Policy Paper No. 7 / December 2017

RISKVIZ

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

The publication "Cyber Insurance as a Contribution to IT Risk Management. An Analysis of the Market for Cyber Insurance in Germany" is based on the publication „Cyberversicherungen als Beitrag zum IT-Risikomanagement – Eine Analyse der Märkte für Cyberversicherungen in Deutschland, der Schweiz, den USA und Großbritannien" by Dr. Constance P. Baban, Tyson Barker, Yvonne Gruchmann, Dr. Christopher Paun, Anna Constanze Peters, Dr. Tim H. Stuchtey, published as BIGS Standpunkt No. 8, September 2017. The study is an outcome of the "RiskViz – Providing a Risk Situation Picture of Industrial IT Security in Germany" project. This project is funded by a grant from the Federal Ministry of Education and Research. We are grateful for their support.

The contents and recommendations of this report were facilitated by resources under program code 16KIS0253 of the Federal Ministry of Education and Research. The authors are solely responsible for its contents.

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

RISKVIZ

BIGS | Policy Paper

Brandenburg Institute for SOCIETY and SECURITY

Cyber Insurance as a Contribution to IT Risk Management

An Analysis of the Market for Cyber Insurance in Germany

Dr. Constance P. Baban, Yvonne Gruchmann,
Dr. Christopher Paun, Anna Constanze Peters, Dr. Tim H. Stuchtey

December 2017

Brandenburgisches Institut für Gesellschaft und Sicherheit gGmbH
Brandenburg Institute for Society and Security gGmbH

Executive Director
Dr. Tim H. Stuchtey

Dianastraße 46
14482 Potsdam

Telephone: +49-331-704406-0
Fax: +49-331-704406-19

E-Mail: info@bigs-potsdam.org
www.bigs-potsdam.org

EXECUTIVE SUMMARY

Digitalization promises enormous gains in productivity but comes with significant cyber risks. In order to make full use of its potential, certain downsides of digitalization need to be properly addressed. This study focuses on one particular aspect of risk management: cyber insurance. It examines the German cyber insurance market in particular and shows potential for significant growth of this market. Yet, a number of factors need to be addressed in order to bolster such growth:

- Calculating premiums is difficult with limited information about cyber risks. The US market shows that reporting requirements can lead to greater risk transparency, which can facilitate the calculation of insurance prices. The German IT Security Law of 2015 introduced reporting requirements for critical infrastructure providers, but their effect remains to be seen. In particular, it is an open question if the information is made available to insurance companies, for example in anonymous form, for a better risk calculation. Increased information-sharing and widening the scope of reporting requirements should be considered if further risk information is needed.

- It is very difficult for customers to compare and find appropriate cyber insurance policies due to information asymmetries and a lack of a common standard. While the latter has been addressed with model conditions published by the German Insurance Association (GDV) in 2017, a further step would be to create a database where potential clients could search for and compare cyber policies.

- Cyber terrorists may attack individual companies, though they target the entire state or society. Therefore, insuring terrorism-related risks needs to be a feasible option. If this is not possible on the insurance market, the state can step in as a reinsurer.

- Cyber insurance can transfer risks to an insurer, but also has the potential to set IT security standards required to get insurance or insurance at a reduced rate, thus increasing security for all members of society. This potential, however, is not fulfilled so far. Risk assessments conducted by insurers are based primarily on potential damages with security measures playing only a minor role or none at all. Attempts to offer lower premiums for customers who comply with security standards were unsuccessful in the UK as the cost of getting compliance certified was higher than savings on premiums. If this gap cannot be closed, the positive externalities from higher security standards would justify the state to step in with financial support for certifications or for the insurance policies that require them.

- The German insurance industry could position itself as a relevant actor on the IT security landscape by adding security assessment components to its risk assessments and putting more emphasis on support services. This would aid clients in preemptively improving their IT security and would offer emergency assistance in the event of a security breach. It would also help insurance companies to gather information about cyber risks and calculate premiums more efficiently.

- German companies remain largely unaware of their own cyber risks, but these risks must become a more important component of overall risk management strategies in order to make full use of the potential of digitalization. Cyber insurance can be an essential part of such strategies and is particularly attractive for the transfer of residual risks if the potential damage is very high and cannot reasonably be covered by equity. However, investments in cyber insurance should not come at the expense of investments in IT security.

FOREWORD

Why is it not possible to obtain insurance for cyber risk in the same way we do for burglary? This question was the starting point of our deliberations. Once one looks into the matter, it quickly becomes clear that some policies are offered by some insurers in a few countries, but that these are often tailored to the needs of large customers and only cover partial aspects of cyber risk. In some countries (e.g. the United States), there is considerable demand for such products, while most insurance policies on the global market for cyber insurance are offered in others (e.g. the United Kingdom). What are the reasons for this? What regulatory framework conditions favor supply and demand in these respective markets? Is it possible to enable the efficient calculation of cyber risk and transfer it into the hands of insurance companies?

In this study, we attempt to look into these questions. First, the role of insurance in managing the economic aspects of cyber risks will be analyzed, with a special focus being on industrial cyber risks. This means that the theft of data via the Internet is not at the forefront of our considerations, but rather the manipulation or even sabotage of industrial production processes through SCADA and industrial control systems.

Industrial processes are being increasingly managed and controlled over the Internet. Industry 4.0 and developments towards an Internet of Things (IoT) are increasing the number of possible attack vectors. This means that, if they wish to exploit the opportunities offered by digitalization without exposing themselves to incalculable risk, corporate management has the fundamental responsibility of economically managing IT security risk. The transfer of this risk to insurers plays a prominent role in efforts to fulfill this responsibility. If such a transfer is not successful, advances in the digitalization of production will also be inhibited.

We discuss the necessity of security standards in the cyber realm and, connected with that, the necessity of government regulation to increase the level of security. Through insurance terms and conditions, insurers can also play an important role as a quasi-regulator in this area and can provide an incentive for the industry to strengthen their security efforts. Whether insurance is taking on this role is an additional question that we also pursue in this study.

This study and the work that went into it would not have been possible without financial support from the German Federal Ministry of Education and Research (BMBF) and its IT Security Research Program. We have learned much about the technical background behind industrial cyber attacks in the project RiskViz – Providing a Risk Situation Picture of Industrial IT Security in Germany – and from our project partners. This background knowledge was needed to take on this task we have set for ourselves. Nevertheless, by no means does this study answer all of the questions related to the insurability of cyber risks. We are therefore hoping for additional support, especially from the BMBF, for our work.

We would foremost like to thank the many people at insurance providers and brokers, industry associations, regulatory authorities, research institutions and security agencies in Germany who allowed us to anonymously interview them. Their knowledge made a crucial contribution to the success of this study.

As authors, we are especially pleased when someone reads this entire study from beginning to end. However, we also believe that it is also possible to read each of the chapters individually. Of course, we would warmly welcome comments or inquiries about the statements made in this study.

Dr. Tim H. Stuchtey

Executive Director

BIGS –
Brandenburg Institute for Society and Security

TABLE OF CONTENTS

LIST OF FIGURES AND TABLES

LIST OF ABBREVIATIONS

BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (German Federal Office for Civil Protection and Disaster Assistance)
BIBA	British Insurance Brokers' Association
BMBF	Bundesministerium für Bildung und Forschung (German Federal Ministry of Education and Research)
BMI	Bundesministerium des Innern (German Federal Ministry of the Interior)
BSI	Bundesamt für Sicherheit in der Informationstechnik (German Federal Office for Information Security)
CI	Critical Infrastructure
CRM	Customer Relationship Management
DESTATIS	Statistisches Bundesamt (German Federal Statistical Office)
DIN	Deutsches Institut für Normung (German Institute for Standardization)
ERP	Enterprise Resource Planning
GDPR	General Data Protection Regulation (of the European Union)
GDV	Gesamtverband der Deutschen Versicherungswirtschaft (German Insurance Association)
ICS	Industrial Control Systems
ISMS	Information Security Management System
IT	Information Technology (including Office IT)
IoT	Internet of Things
ISO/IEC 27001	International Organization for Standardization / International Electrotechnical Commission Requirements for Information Security Management Systems
NIS Directive	Directive on Security of Network and Information Systems
OT	Operational Technology (including Production IT)
SCADA	Supervisory Control and Data Acquisition
SMEs	Small and mid-sized enterprises

I INTRODUCTION

1. Background

Numerous national and international cyber attacks and the damage they have caused show that the management of IT risks must become an increasingly important component of corporate management. For example, in 2017, for the first time the Allianz Risk Barometer came to the conclusion that cyber risks represent the largest risk for companies in Germany.[1] In 2013, however, cyber threats did not rank amongst the top 10 business risks.[2] If we look at the damage figures associated with cyber attacks, they at first tell us little. In its 2015 annual report on the state of cybercrime in Germany, the *Bundeskriminalamt* (Federal Criminal Police Office) specified damages of 40.5 million EUR.[3] However, we must assume that, due to the large number of cyber attacks that are not criminally prosecuted, actual damages far exceed this. For example, for the years 2014 and 2015, KPMG cites estimated damages of 54 billion EUR to the entire German economy.[4]

In addition to the risks and potential damages related to office IT that companies are subjected to, such as those related to data theft, there is one field of IT security that so far has received much less attention: production-related IT, for example industrial IT security. Industrial production is generally characterized by IT risks throughout the automatization pyramid, specifically the use of industrial control systems (ICS) and, as part of these, supervisory control and data acquisition (SCADA) systems, with which production processes are implemented, controlled and monitored.

The use of such systems is not new. They have been in existence to some degree for over 20 years. However, what is new is that they are increasingly networked, that is, connected to the Internet. The reasons for this include, for example, more cost effective ways to remotely access and maintain these systems. However, this entails new security risks for companies, as large numbers of these networked control systems are unprotected and can be attacked over the Internet. The German Federal Office for Information Security (BSI) accordingly notes the existence of this new threat as follows:

"Systems for the automatization of production and processes – referred to by the term Industrial Control Systems (ICS) – are used in almost all infrastructures that conduct physical processes. These range from energy generation and distribution to gas and water supplies and on to factory automation, traffic management and modern building management. Such ICSs are increasingly exposed to the same cyber attacks as conventional IT." [5]

The consequences of a cyber attack on an ICS can range from sabotage and espionage to the interruption of entire production processes or the destruction of facilities. For the industry, this kind of damage can be tied to high financial losses. This fundamentally applies to all businesses. However, for businesses that, according to the 2015 German law to increase the security of information technology systems (IT-Sicherheitsgesetz or IT Security Act) fall in the category of so-called critical infrastructure (CI), that is, infrastructures which are considered to have special significance because they supply utilities that are required by society to function, the situation has the potential to be much worse. According to a definition of the German Federal Ministry of the Interior (BMI), critical infrastructures are described as follows:

"Critical infrastructures are organizational and physical structures and facilities of such vital importance to a nation's society and economy that their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences."[6]

The BMI specifies a total of nine critical infrastructure sectors (Figure 1). The IT Security Act addresses all of these, except for State and Public Administration as well as Media and Culture.

Figure 1: Critical Infrastructure Sectors in Germany

Critical Infrastructure Sectors	Industries
Energy	Electricity, petroleum, natural gas
Food	Food industry, food trade
Health	Medical care, pharmaceuticals and vaccines, laboratories
Information and Communication Technology	Telecommunications, information technology
Finance and Insurance	Banks, insurers, financial service providers, exchanges
Media and Culture	Broadcast (TV and radio), printed and electronic press, cultural heritage, emblematic buildings
Government and Administration	Government and public administration, parliaments, judicial bodies, emergency and rescue services including disaster response
Transportation	Aviation, ocean shipping, inland waterway transport, railway transport, road transportation, logistics
Water	Public water supply, public wastewater treatment

Source: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2014); own figure.
(German Federal Office of Civil Protection and Disaster Assistance)

A cyber attack on a critical infrastructure can result in higher financial losses on the one hand, and on the other hand, sabotage or the disruption or destruction of a critical infrastructure can also have life-threatening consequences for the society as a whole. From the perspective of potential attackers, critical infrastructures can also be a more attractive target for an attack, because of its criticality. One example in this case would be the global cyber attack on remote access ports of DSL routers in November 2016 that cut Internet access for 900,000 Deutsche Telekom customers.[7] Had this global attack been successful, it would have become a national security problem for Germany. The identification of gaps in the protection of ICS systems, as well as the development of appropriate protection strategies, is therefore not only essential for risk management in the industry and the economy in general, but also for operators of critical infrastructure.

The research project RiskViz – Providing a risk situation picture of industrial IT security in Germany – takes up this issue. The project's foundation is the development of a search engine whose purpose is to identify potentially vulnerable ICS systems connected to the Internet. The search engine developed during the project makes it possible to identify potentially vulnerable industrial control systems on the Internet, serving as a possible early warning tool for the recognition of industrial IT risks. Over the long term, the aim is to ensure the use of this search engine by businesses and public authorities. This would be beneficial for several actors in the IT security landscape. First, for companies that use ICS for their production processes, information about such risks could serve as a component in their IT risk management process. Additionally, the aggregated visualization of potentially vulnerable ICS in Germany would provide additional information for situation reports, like those regularly produced by the Federal Office for Information Security (BSI).

Even when ICS are sufficiently protected by identifying vulnerabilities and implementing appropriate countermeasures, a full protection can never be guaranteed and some risk will always remain. For the companies concerned, whether they are critical infrastructure providers or not, the question remains of how to deal with this remaining risk. Therefore, within the scope of the overall RiskViz joint project, cyber insurance and the industrial IT security of critical infrastructures are one focus of the BIGS subproject. In civil security in Germany, the IT security of CI plays a role that is special compared to that of other

companies, because the failure of CI, for example as a result of sabotage or destruction, could have severe consequences. At the same time, CI scenarios that could result in the loss of life are also conceivable.

Whereas a "functioning" cyber insurance market has existed in the United States since the 1990s – at least as far as cyber risks related to data access are concerned[8] – the general cyber insurance market in Germany is only slowly gaining momentum. Nevertheless, the revenue figures presented in this study confirm that cyber insurance is a growing market, nonetheless revenues measured in absolute terms in Germany are still low in this field.

2. Structure

This study is based on the hypothesis that the full potential of production advances due to digitalization can only be tapped if the cyber risks associated with them can be controlled as part of corporate IT risk management. Cyber insurance can play an important role in this context (see Chapter II, Section 2). The question of the insurability of cyber risks is fundamentally embedded in the larger context of how society as a whole deals with cyber risks and the matter of risk distribution. Chapter II will be expanded to include a short clarification of the terminology related to IT security (Chapter II, Section 1).

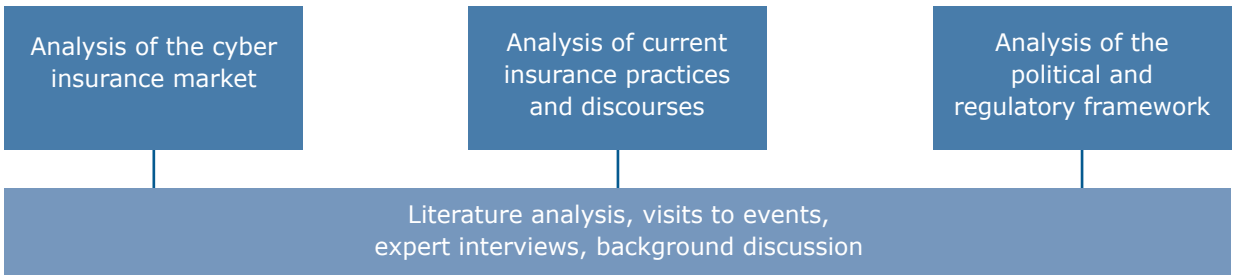
The research goal of this study is a comprehensive analysis of the German cyber insurance market in particular as well as the insurability of industrial IT risks – including critical infrastructure risks (Chapter III). After starting with a description of the current cyber insurance market (Chapter III, Section 1), the market barriers in the German market in general as well as for the critical infrastructures in particular will be identified in the following section (Chapter III, Section 2). Building upon this, factors that could positively influence the German cyber insurance market will be outlined (Chapter III, Section 3).

In the final chapter, a conclusion will be drawn and recommendations for actions that policymakers, the insurance industry and individual companies can take to further develop the German cyber insurance market will be made (Chapter IV).

3. Methodological Approach

Particularly in regard to Germany, the development of the cyber insurance market and the fundamental question of the insurability of cyber risks, including in the case of critical infrastructures, is a very new, perhaps even largely unexplored field of research. It was therefore not possible to draw upon an extensive pool of scientific literature for this study. This is also the case for the IT Security Act, which is currently still in the process of implementation. For these reasons, this study is the result of an interplay of background discussions, expert interviews, visits to conferences and events, and the evaluation of available literature and documents. In addition, qualitative semi-structured interviews were conducted with various stakeholders in the fields of insurance and reinsurance, insurance brokers, public authorities, industry associations, research institutions and private companies in Germany. However, exchanging information about cyber insurance proved easier to accomplish with representatives from the insurance industry and public authorities than with companies and CI operators. This is partly due to the novelty of the topic of cyber insurance and a fundamental sensitivity about external communication, especially where questions of corporate security and IT security are concerned. Conversations with company representatives at events, some of which were confidential, were more helpful in grasping the subject in all its complexity.

Figure 2: Methodological Approach



Source: Own figure.

II THE CONNECTION BETWEEN IT SECURITY AND CYBER INSURANCE

1. IT Security between Information Technology (IT) and Operational Technology (OT)

To better understand the function of cyber insurance as it relates to IT security in companies, it is first important to define the key terms. In general, the term cyber security has become widely used internationally to describe the security of information technology systems and the three protection objectives – integrity, confidentiality and availability.

However, the use of the term cyber security (Cybersicherheit in German), which in Germany primarily has its origins in the political sphere, is regarded with a certain amount of criticism within the IT scene and is somewhat considered overly fashionable. However, once we ignore differences over the use of the terms "IT security" or "cyber security" and agree that both terms are intended to describe the same thing, the question remains of what we are exactly referring to. Within this study, following the BSI definition, IT security and cyber security are understood as:

"Cyber security concerns itself with all aspects of security in information and communications technology, thereby expanding the field of action of classic IT security include all of cyberspace. This includes all information technology connected to the Internet and comparable networks and all communications, applications, processes and processed information based upon this technology."[9]

Building upon this, we can explain the distinction between IT and OT:

"'Normal' IT is a landscape consisting of workstation computers with the classical office applications, mobile devices and server systems like CRM and ERP. These systems can be grouped together under the term office IT. The situation in production is similar, where control terminals are based on classical desktop operating systems. Analogous to office IT, these systems are called production IT."[10]

Industrial control systems are classically included as part of OT. However, the criticality and thus also the vulnerability of the production systems are a result of the increasing convergence between IT and OT. Thus, today, IT and OT can hardly be regarded as independent from one another, due to their networked character.[11] It is even plausible to suggest the thesis that "there will no longer be several separate IT worlds, but rather in the future only one."[12]

Efforts to implement cyber security and the question of how to calculate cyber risk and deal with it must therefore always take both of these dimensions of IT security into account. However, all things considered, it is difficult to draw a clear, ad hoc distinction between critical infrastructure operators whose office IT should be protected and

those whose production IT should be protected, or even those for whom both areas need protection. This would require an extensive assessment review based upon the IT Security Act and critical infrastructure operators (see also Chapter III, Section 3.2).

To develop the economic understanding of cyber security that is also necessary within the context of this study, the BIGS definition of security will be drawn upon, according to which security is a function of threat and degree of protection.[13] Within this framework, residual risk is thus always risk that remains after a company has taken all intended protective measures. The extent of this residual risk then depends upon the scope of existing protective measures and the given threat. This understanding of security illustrates why, despite protective measures, there is a remaining risk that may have to be insured against.

The individual scientific disciplines have different views of risk and have no uniform definition for risk.[14] The classic economic definition views risk as a result of the multiplication of potential damage by the probability that such damage will occur. Hence, this also applies to cyber risk.

In contrast to the example of a flood, which can be relatively reliably measured thanks to long-established centralized flood registries with probability calculations, estimating the likelihood of a successful cyber attack is more difficult. This likelihood not only depends on which attack methods are currently the most common, but also the vulnerabilities of the target company. These can include not only technical weaknesses, but also patterns of employee behavior. However, a high calculated risk can have two different causes: in one case, it may be a low level of potential damage (loss) with a high probability of occurrence; in another, it could be a high level of potential loss with a low probability of occurrence. For cyber insurance – the focus of this study – in addition to the cyber risk, which is understood as the result of multiplying the possible loss by the possibility that the loss will occur, the determination of the potential size of the loss within the company is crucial. This admittedly poses currently one of the most important challenges.[15] The damage or loss potential and especially the conversion of the cyber damage into a monetary figure is the basis that the company uses when planning how to deal with the potential financial loss. When that is accomplished, one of the components to deal with the management of cyber risks can be a cyber insurance.

2. The Influence of Cyber Insurance on the Level of IT Security in the Company

The most important characteristic of cyber insurance is that it transfers the financial risk of a cyber attack or cyber related loss in general to an insurance company. In this study however, we want to take a somewhat broader view of cyber insurance, rather than "only" considering it from the risk transfer perspective. Instead, we regard cyber insurance and thereby the insurance industry in Germany as a whole as an important actor in cyber security in Germany. This attribution is based on the considerations about the connection between cyber insurance and the level of IT security in a company. If we consider the influence of cyber insurance on the level of IT security at an individual company, we can initially conceive of three reasonable possibilities for how this influence could be interpreted. These are that cyber insurance has

- a positive effect,
- a negative effect or
- no effect

on the level of IT security at a company.

In the following section, the most important lines of reasoning for these three possibilities will be outlined.

The starting point for this study is the first of these possibilities, namely that cyber insurance could positively affect the level of IT security of

businesses. Fundamentally, insurance is ascribed a central role in the IT risk management process, as with technical security precautions.[16] This means that cyber insurance does not replace other IT security measures, whether they be technical or non-technical in nature, but rather complements them.

If cyber insurance is understood to be one part of IT risk management within a company, then this is because it makes it possible to transfer potential financial losses connected to cyber risk to an insurer. The cost of the insurance policy is the price for this transfer. The insurer can pool the cyber risks of different companies and thus benefit from the law of large numbers. In ideal cases, and depending on the potential extent of the loss and the corresponding coverage provided by the insurer, the provision of insurance for cyber risks should be tied to a risk assessment conducted in advance. Assuming that the issuance of the policy itself and the premium can be tied to the level of security at the company, at this time the company must consider and address its own level of IT security. At the same time, within a broader framework, the insurance policy should be tied to a regular security inspection. This of course requires us to assume that the company management wishes to purchase cyber insurance. Nevertheless, this represents the ideal situation for the interpretation that the influence of cyber insurance will have a positive effect upon the IT security level of a company.

Conversely, the moral hazard phenomenon leads us to the second possible interpretation, that cyber insurance could have a negative effect upon risk aversion at the company or among its employees. The moral hazard concept explains that, because insurance would cover the losses in the event they occur, this leads to riskier behavior. Put simply, if you have cyber insurance, you no longer need to worry about IT security and can accept greater risks, because if something should happen, the insurance will pay for it. The same is true when the resources that were invested in a cyber insurance policy are no longer available for investment in IT security measures.

Finally, it can be postulated that cyber insurance has no significant influence on the level of IT security at a company. Some studies for the US market seem to support this idea.[17] We could assume that this applies when companies can already demonstrate a high level of IT security, either as a result of their own initiative or as a result of external regulation, so that cyber insurance can have no additional influence on their IT security. Beyond that, the insurance transfers the remaining risk to the insurance company in the event of a loss due to a cyber attack anyway.

The other case in which cyber insurance would not have an effect would be if the initial level of IT security at a company were very low, and the issuance of a cyber insurance policy is not tied to adjustments in the security level. The company thus relies only upon the protection provided by the insurance policy, but behavior that is less risk-averse is not encouraged. Because IT security is a responsibility that is never permanently fulfilled, but rather one that grows dynamically as technology changes, a lack of influence cannot be considered good per se, as it can still lead to negative effects.

These three possible interpretations clearly illustrate the two different functions that cyber insurance can perform in regard to an IT risk management strategy: on the one hand the transfer of the residual financial risk to the insurer, and on the other hand the improvement of the level of IT security, when the insurance is tied to security conditions. To better understand the functional quality of a cyber insurance policy as part of the risk management of a company, we can consider cyber insurance in relation to other IT security measures.

Explained in simple terms, this is possible if IT security measures are associated with a loss event and if they are divided into preventive and reactive measures. A cyber insurance policy would then be considered a reactive measure that takes effect when a cyber incident occurs. Preventative measures could include, for example, technical security precautions or employee training. These could be implemented through the observance of specific standards and certification measures, for example, and could also be included in the conditions of the security policy. Depending on the context of the insurance, a policy could therefore only perform a reactive function, or could perform equally reactive and preventative functions within the framework of a corporate IT risk management process.

III THE CYBER INSURANCE MARKET IN GERMANY

1. Description of the Market

This section provides an overview of the German cyber insurance market. To do this, it is necessary to look at the insurance market as a whole, as there is not yet a distinct and separate market for cyber insurance. The ways in which cyber risk has been addressed by insurers to-date, as well as unresolved questions related to the structure of the traditional insurance market as it has developed over time will be identified.

The introduction will address the specific situation of cyber risk within the insurance market and its economic significance. The product classification scheme that follows is country-specific and will only be explained for Germany. This is followed by the quantification of the single (exclusive) cyber insurance policies offered in the German market as well as key figures and prognoses for the German cyber insurance market.

1.1 The Specific Situation of IT Risk – The Controversy

Since 1994, the implementation of European legislation has led to the far-reaching deregulation of the insurance market and consequently to more competition within Europe as well as to a concentration of insurance providers. In addition, as a result of banking and financial crises, the capital requirements and risk management stipulations for financial service providers have been increased.

Currently, the cyber insurance market is dominated by international insurers, who are able to profit from their size and their experience, especially in the United States. What actually should be considered cyber insurance is a subject of controversial debate within the industry. The spectrum ranges from cyber insurance as an independent product (stand-alone policies) to the integration of cyber risk into classic business policies via the provision of such coverage through additional modules that are added to existing policies.

The introduction of stand-alone cyber insurance is frequently met with skepticism; instead, the case is often made for the implementation of add-ons within conventional policies. In contrast, many of the experts interviewed for this study (see Chapter I, Section 3), were in favor of drawing a distinction between cyber risk and other business risks by creating a completely new product line. It is still absolutely unclear which of these two possibilities will establish itself in the market in the end.[18] As will be shown in Chapter III, Section 1.3, the landscape of insurance contracts is currently very heterogeneous, even among stand-alone cyber policies.

The difficulty of calculating cyber risk is a factor that supports the distribution of this risk into a pool of pre-existing insurance policies that is as large as possible. Within such a diverse pool of different risks, it would be easier to distribute the new (cyber) risk among the large numbers of policyholders. Furthermore, existing policies have longer contractual periods, meaning that risk can also be spread over a longer period of time. In this way, individual risk drops considerably and the risk community can bear the risk in the pool until it is possible to make better predictions about the actual likelihood and extent of loss from cyber risk. If the same kinds of IT risks can be clustered together over the course of such a process, it would then be possible to insure these within their own product group and thereby establish an independent product line.

The most important argument against such an approach is based in the high cumulative risk of IT-related risks. This cumulative risk is rooted in the fact that the high degree of interconnectedness between many companies' IT means that damage from a cyber attack can spread virally among them, suddenly resulting in an excessive accumulation of claims within the risk community. In such a situation, existing risk pools which had functioned well up to that point would then fail and dissipate, leading to a drop in the level of insurance protection.

Stand-alone cyber insurance has existed since the 1990s and has been available on the insurance market in Germany since 2011. Especially

since 2014, offers of stand-alone cyber insurance policies have increasingly been appearing in insurers' online product information materials. A regularly updated overview of the policies that are publicly available can be found in Chapter III, Section 1.3. Observations in the following section will be limited to Germany, but can be viewed as being generally representative of the European insurance market as well as of those cyber insurance policies available as stand-alone policies on the open market.

1.2 Cyber Insurance within the Broader Insurance Market

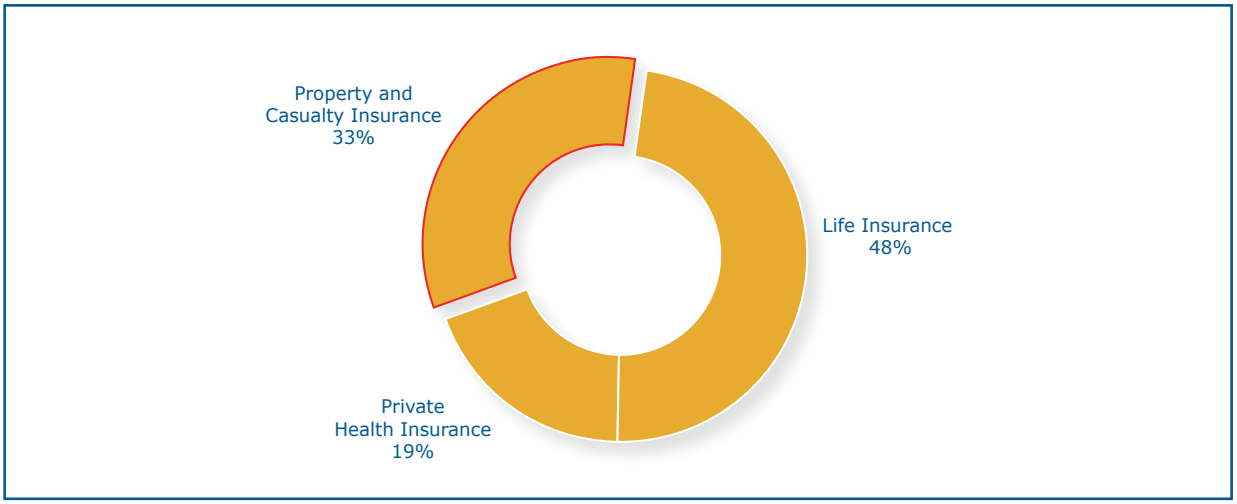
In 2016, the volume of premiums for the entire primary insurance market in Germany totaled 194 billion Euros.[19] However, we must ask what proportion of this market is of interest for cyber insurance and what premium potential can be expected from a cyber insurance segment in the future. To answer this question, it is necessary to first take a look at the product structure of business insurance that is potentially relevant for IT security[20], and especially at industrial insurance.[21]

1.2.1 Business Insurance

The entire volume of the insurance market in private and business insurance is comprised of the following insurance segments: life insurance, health insurance and property and casualty insurance. Whilst the life and health insurance segments are dominated by insurance for private individuals, in the case of property and casualty insurance, the customer portfolio is more mixed and requires a more differentiated examination. Aside from all of these areas, there is also the reinsurance market, which will not be considered here. The property and casualty insurance segment is the one that addresses the IT risk of businesses. This segment currently accounts for about one third of all insurance premium revenues (66.2 billion EUR).[22] The cyber insurance potential of private insurance in the property and casualty segment will not be considered here. However, it is extremely difficult to separate out business insurance[23] and its premium volume.

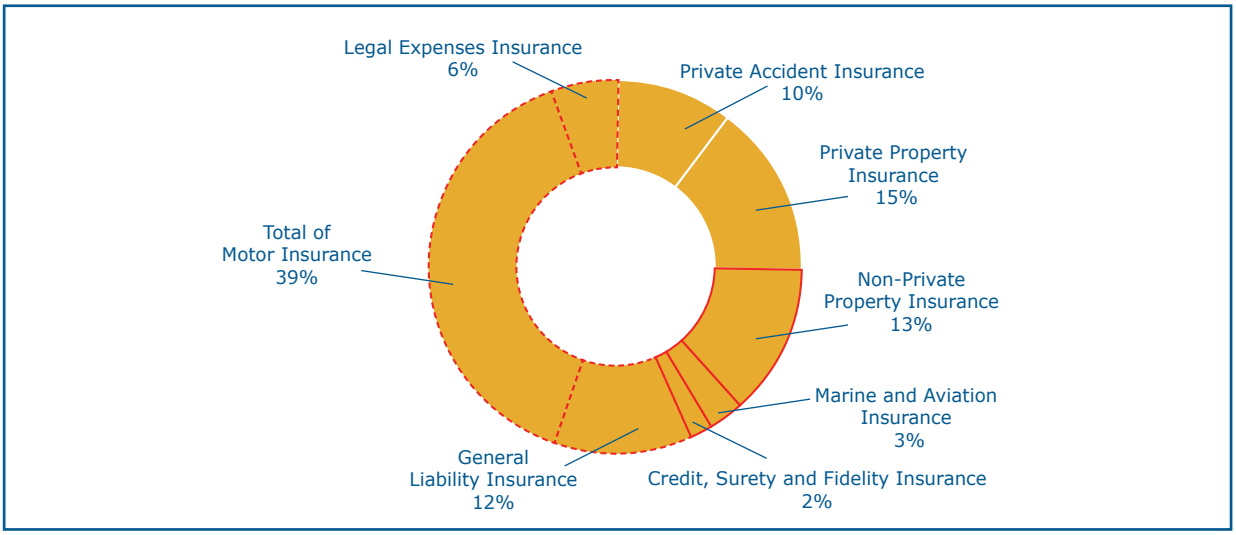
If one consequence of increased interconnectedness is that potential damages associated with conventional business risk can also be generated by IT risks, potential damages due to a cyber attack would also fall within the known spectrum of possible damages within the category of business property and casualty insurance. If we accept the estimates of a KPMG study and include the private insurance segment in our calculations, the cyber insurance portion of the property and casualty segment would currently account for 1.4 percent of total premium volume, rising to around 20 percent in 20 years.[24] This means that the cyber insurance portion of this segment should grow by an average of 15 percent annually.

Figure 3: Segments by Share of Premium Revenues, 2015



Source: Own figure based on GDV (n.d.)(1).

Figure 4: Property and Casualty Market by Share of Premium Revenue, 2016*



Source: Own figure based on GDV (n.d.)(2); *preliminary figures.

1.2.2 The Special Case of Industrial Insurance

Whereas industrial insurance primarily covers risks with high loss potential and lower frequency of loss, business property insurance covers smaller but usually more common potential losses, especially for small and mid-sized enterprises (SMEs). Cyber insurance policies can essentially be found in both categories. However, cyber insurance policies for SMEs have just recently begun to be offered. In contrast, in industrial insurance, an appreciable number of cyber insurance policies are already available.

The basic structure of a comprehensive insurance protection for a business consists of first-party insurance, third party insurance, and special insurance for special risk groups for whom the previous distinction does not apply. First party insurance includes the fields of property insurance and engineering insurance. In contrast, third party insurance includes industrial liability insurance and financial lines insurance. Special insurance appeals to clearly defined policyholder groups, such as air transport operators or shipping companies in multiline products.

Figure 5: Components of Industrial Insurance

First Party Loss	Third Party Loss	Special Insurance
Industrial property insurance: • Fire insurance • Extended coverage insurance • Insurance for business interruption due to fire **Technical insurance:** • Construction and assembly works insurance • Machinery breakdown insurance • Financial loss insurance	**Industrial liability insurance:** • Business risks, e.g. business liability insurance • Environmental risks • Recall risks **Financial lines:** • Directors & officers insurance • Criminal defense insurance	**Aviation insurance:** • Aviation hull insurance • Aviation accident insurance • Aviation liability insurance **Transport insurance:** • Hull insurance • Cargo insurance • Transport liability insurance

Source: Own figure.

Conventionally, insurance that covers losses by the policyholder has been handled separately from insurance that covers third party losses, due to the different types of losses.

In the case of a loss resulting from a cyber attack, there are both first and third party property and financial losses. Thus, under traditional insurance practices, it would be necessary to obtain multiple policies to provide protection. If several types of loss are covered by one policy, that policy is known as a multiline policy. Multiline policies cover first and third party losses and property and financial losses. Special insurance policies offer such multiline coverage, but only for very specific groups of policyholders. However, digitalization and therefore cyber risk affect all economic sectors and thus cannot be tied only to selected customer groups. Thus, the categorization approach used above (separating industrial insurance into segments), does not allow us to cleanly classify cyber insurance policies; this would require the development of cyber insurance into an independent class of products.[25] A dominant view about the classification of cyber insurance has yet to become established within the broader business insurance community.

1.2.3 The Role of Insurance Brokers

As the diversity and lack of clarity in the structure of business insurance described above would lead us to suspect, there is very little transparency. Especially in the field of business insurance, this lack of transparency has led to the establishment of a group of intermediaries who assist customers seeking to buy policies. It would be hard to imagine a functioning insurance market without the expertise of insurance brokers for certain risk areas and customer groups, such as Marsh, Schunk and Aon. In the cyber area, brokers often provide consulting services and manage the contract initiation process. These brokers have a knowledge advantage that includes bundling knowledge from the policyholder about new IT risks, loss scenarios and the extent of losses that have occurred, as well as the bundling of knowledge about the heterogeneous policies offered by the insurers.

This knowledge advantage on the part of specialized brokers reduces transaction costs. In addition, in the course of the consultation process, an initial risk engineering effort is undertaken, usually as a fee-based additional service.[26] It is currently almost impossible for potential customers to gain an understanding of the differential structure of premiums or the scope and quality of the coverage services available before signing a contract (see Chapter III, Section 2). Brokers are also considered to have an arbiter function, which can be called upon in the case of incomplete contract stipulations.[27] In the extremely dynamic field of cyber threats, this means that a broker can support dynamic adjustments to a contract.

1.2.4 Conclusions on the Structure of Insurance Products and Economic Relevance of Insurance

The fundamental fact remains that the economic significance of the insurance industry is greater than the quantifiable volume of business insurance premiums alone (see also Chapter II, Section 2). Often, business operations are only possible once the risks not associated with the company's central purpose have been transferred, thereby evening out the balance sheet. Only once these risks are pooled, does it become possible to calculate them. This especially applies to risks that are new and difficult to predict, such as those that come with digitalization. The opportunities of digitalization can only be realized for companies once it is possible to transfer this risk to insurers. This fact does not only apply to cyber risk, but is especially significant in a phase of radical industrial change, unleashed by the transformative process of digitalization.

1.3 The Modular Structure of Stand-Alone Cyber Insurance Policies

The cyber insurance policies available on the market today include the following coverage in the event of a loss (see Chapter III, Section 1.2):

- coverage of first party losses,
- coverage of third party losses and
- support services.

First party losses as a result of a cyber attack can include, for example, when business opera-

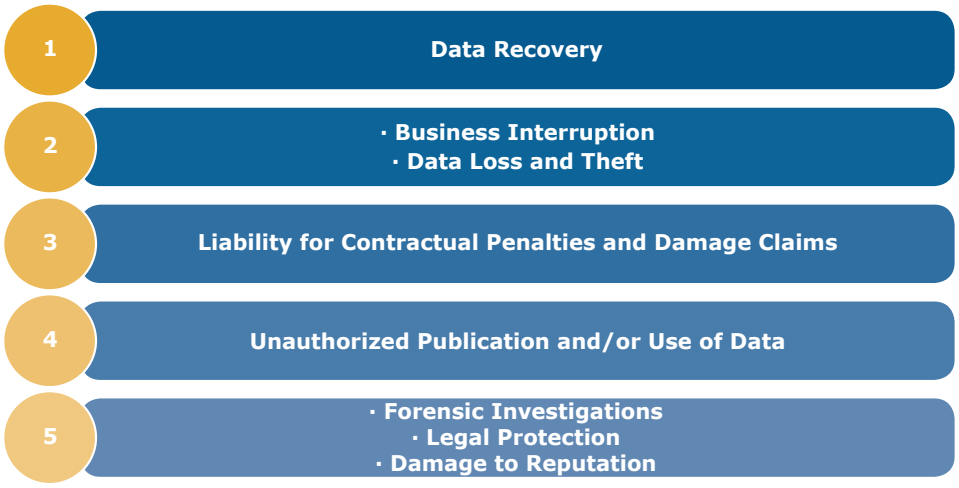
tions are interrupted or financial damages tied to ransom demands. But property damage is also conceivable – as demonstrated by a hacker attack in 2014 which was able to gain control of a blast furnace at a steel mill, thereby seriously damaging the facility.[28]

If an attack on an IT system results in losses to third parties, these could also conceivably be in the form of personal injury or property damage or financial losses. Solutions to address all of these categories are available on the open market. Coverage modules such as data recovery, special legal expense insurance and packages that inform customers affected by data theft and limit their liability can be flexibly combined. The current practice is to assign different coverage limits to the individual coverage modules. However, the extent of legal liability to third parties is still unclear to a large degree and must first be interpreted in court decisions.

The third package of services includes the limitation of first and third party losses in the event of a cyber attack through preventative risk analyses, early recognition and response to attacks, and criminal prosecution. These services can be optionally expanded to include more extensive support services, for example establishing contact to experts in crisis management, public relations and IT forensics.

Attempts to develop a current overview of the coverage modules that are actually included within cyber insurance quickly encounter several barriers due to the modular and individualized design of the policies. An analysis of the cyber insurance policies currently offered by about 20 providers in Germany is able to identify the following commonly used coverage modules. These are listed in figure 6 below in order of their frequency.[29]

Figure 6: Modular Structure of Cyber Insurance Policies



Source: Own figure based upon the BIGS cyber insurance policy database, February 2017.

This overview makes it clear that to date, data modules – positions 1, 2 and 4, namely the abuse, loss and recovery of hacked policyholder and customer data – have often been addressed, but differently. Furthermore, in these cases, depending on the kind of data, international empirical information is available that makes it possible to more exactly specify potential damage and thereby calculate it. Thus, for example, the black market price for a complete data set for a credit card ranges from 30 to 45 USD.[30] However, the adjustment of a data theft claim with both direct costs, such as informing the owner of the credit card[31], and indirect costs, such as losing customers, costs 150 EUR[32].

Ranked second is the business interruption module. This module includes damages that reach into the physical plant of a company. Here too, empirical data is available about the potential losses

due to an interruption of operations caused by classical risks such as fire and supply chain bottlenecks and the lost production that they cause. Property damage and revenues are the basic parameters used to estimate losses. However, it is not yet possible to predict the probability that such damages can result from a cyber attack, which makes it more difficult for insurers to calculate premiums.

Furthermore, as the module in third place shows, new risks are arising due to changes in legislation affecting the contractual penalties and compensation rights of third parties. For example, the European General Data Protection Regulation specifies damages for the violation of data privacy of up to four percent of the global annual revenue of a company.[33] However, as long as these legal regulations are inconsistently applied, insurers' calculations, which are based on obligations specified in the American regulatory frameworks, may be too high.[34]

The fifth rank is held by coverage modules that all consist of support services provided by the insurer and whose goal is mainly to limit losses after an attack. Expert knowledge that the insurer has collected and/or cooperation agreements with IT service providers, such as the cooperation agreement between Hiscox and HiSolutions, can bundle important findings about the exact source of threats, due to the widespread use of these modules. However, due to a lack of experience with losses by policyholders, it remains to be seen how large demand for these modules will be.

The short look at the coverage modules currently offered by insurers illustrates the uncertainties that exist even within the scope of possible damages that can be defined. This uncertainty can – to the extent that some empirical data are available – be limited by excluding some insurance benefits or limiting claim amounts.

In the German cyber insurance market, maximum coverage amounts of 100 million EUR per policy are available, in combination with maximum coverage amounts per coverage module. Furthermore, losses or abuse of personal data tied to a bank or credit card can be limited to a fixed amount per data set. Coverage exclusions may be contractually agreed upon if cyber incidents occur repeatedly. These risk limitation instruments are widespread in the industry and will only decrease in number as experience with loss cases grows.

Another avenue of reducing policyholder risk is the requirement to fulfill certain security guidelines and/or to take steps to prevent damages. Minimum technical standards common in the industry are often used. The installation of smoke detectors at a business as a minimum standard to purchase fire insurance would be an analog example of such standards. Similarly, the observance of IT risk management procedures could be seen as a requirement for obtaining cyber insurance. Commonly required measures could also include regular security updates, encrypted data transfer or an external IT security inspection. In addition, the industry and size of the respective company, its exposure and any geographical special features could play a role, as could the size of the insurer.

Fundamentally, such cyber insurance should consequently offset a reduced crisis management budget as well as first and third party damages, and should also provide some crisis management in the form of the support services mentioned above. Here it is essential to make distinctions based on the size and type of business in question. Large companies almost always have an extensive crisis management team which they can activate if needed. These teams include IT experts, legal advisors and public relations managers. Larger companies are also more attractive for criminal attacks, because their higher revenues increase their ability to pay large sums.

At the same time, medium sized companies are becoming increasingly attractive as the costs of carrying out an attack continue to fall. Their frequent lack of IT experts suggests a lower level of protection, so attackers believe that less time, effort and expert knowledge is needed to be successful. In the future, smaller companies will also increasingly find themselves in the crosshairs of attackers.

Thus, a cyber insurance policy should provide more or fewer support services, depending on the size of the company holding the policy. Depending on the business sector of the policyholder, distinctions must be made based on special pro-

tection requirements for customer data and financial information; examples would be online retailers or companies with high innovative potential. Last but not least, the extent to which the company's IT is networked with other companies (and logistics chains) and social sectors (such as critical infrastructure) also plays a decisive role.

The requirements above are also addressed by the cyber insurance model terms adopted by the German Insurance Association (GDV), published in April 2017,[35] which specify four business risk classes. Depending on the risk class, the risk inspection that is carried out before the insurance contract is signed ranges from simple to complex. The publication of the terms is intended not least to reduce the general uncertainty among insurers, but especially to establish more transparency in this area, as a counterweight to the broad diversity of policies that currently exists (see Chapter III, Section 1.4).

1.4 The Cyber Insurance Market in Figures

Germany is the world's third largest market for non-life insurance.[36] Penetration of insurance services is very high, but because of the positive economic developments and the continual creation of added value there is a constant need to supplement existing insurance coverage. Interest from international insurance providers in new market segments in the German market is naturally very high. In the United States, cyber insurance is already an established component of companies' insurance portfolios. If this development is repeated in the world's third largest insurance market, no one wants to be left out. The current range of offerings is thus dominated by international insurers.[37]

1.4.1 Cyber Insurance Policies Available

The first cyber insurance policy in Germany was offered in 2011.[38] Since then, this new market is considered to have great potential for the future, even if developments in regard to cyber insurance policies purchased continue to make only slow progress. Whereas in 2014, 12 (of approximately 200) federally regulated insurers[39] that offered property and casualty insurance offered a cyber insurance policy on the open market, in early 2017 the number had risen to more than 20.[40] Insurers are also increasingly offering cyber insurance policies to private customers.[41] Also new is the fact that three insurers providing insurance to business customers limit their activities to the German market. Until 2016, insurers without experience in the English-speaking world did not venture into this market. Table 1 lists the active providers of cyber insurance policies and brokers listed in the BIGS cyber insurance policy database through July 2017.

Currently, standard cyber insurance policies do not include all risk coverage. Rather, individual risks (named perils) are specified and coverage for these risks is pieced together modularly (also see Chapter III, Section 1.3). To do this, insured events, such as protection for first party damages related to information costs, the interruption and restoration of business operations, computer fraud and cyber extortion (coverage modules), including the definition of these terms (clauses) and conditions (exclusions and obligations) are defined. In this way, damages due to software that has not been updated can be excluded, for example. This complexity and the modular structure of cyber insurance policies makes a comparison of the policies available difficult.

Table 1: Providers of Cyber Insurance Policies in Germany

Insurance Provider	Cyber insurance policies offered in Germany	Geographic scope and cyber coverage limits
ACE[42]	see Chubb Limited	
AIG	Cyber Edge (2012) Cyber Edge 2.0 (2014)	Global CV in Germany: up to 25 mil. EUR
Allianz Group AGCS[43]	Cyber Protect Premium/Plus (AGCS 2013) Cyberschutz (Allianz 2016)	Global CV in Germany in industry: 100 mil. EUR
AON*	customized policies	Global
ARAG	ARAG Cyberschutz, ARAG Cyberschutz Plus (2017)	Germany CV up to 250.000 EUR
AXA	Cyber Sphere (2011 and 2013) ByteProtect (2014) ByteProtect 2.1 (2015)	Global CV in Germany: up to 25 mil. EUR
Chubb Limited[44]	Data Protect /Plus (ACE 2011) Cyber Security (Chubb 2012) AVB 2015 (ACE 2015)	Global CV in Germany: up to 50 mil. EUR
CNA	Net Protect (2012)	Global IT industry only
Dual	AVB Cyber Defence (2015)	Germany, Austria, Switzerland
Ergo[45]	Cyber insurance /Kompakt (2016)	Europe
Funk	Cyber Secure (2016)	Global
Gothaer	Cyber policy (2017)	Germany, Poland, Romania
HDI	Cyber+ und Cyber+ Smart (2013)	Global Coverage for SMEs
Hiscox	Cyber Risk Management (2011) Cyber Risk Management 2.0, IT liability insurance, Cyber insurance (2015)	Global CV in Germany: up to 25 mil. EUR CIE in 2015: 345 Cooperation with HiSolutions
Kiln Europe[46]	Cyber ProTec (2016)	Europe
Lloyds	various (since 1990)	Global
Markel	Pro Cyber (2016)	Global CIE in 2015: 20-25
Marsh*	Cyber Risk Police (2012)	Global
Munich RE	Cyber Risk Solutions (individualized, 2013) in cooperation with Beazley (2016)	Global CV in Germany: 100 mil. EUR
Schunk*	Schunk Net Risk (2013)	Especially for logistics firms
SentinelOne**	Cyber Warranty (2017)	USA, Israel, Germany, France, Japan
Sparkasse	IT policy (2016)	Germany IT industry only
Swiss Re	Cyber Solution Germany (2016)	Global Cooperation with IBM
Württem-bergische	Cyber Police (2014)	Deutschland CV for SMEs
XL Catlin	XL Eclipse 2.0 (2012) Plc (2013) XL Eclipse 2014 (2014)	Global CV in Germany: up to 25 mil. EUR
Zurich	Cyber Security and Privacy (2013) Cyber & Data Protection (2014)	Global CV in Germany for SMEs: up to 25 mil. EUR

*Broker; **Security Provider; PV: Premium Volume; CV: Coverage Volume; EM: Employees; CIE: Cyber Incident Experience;
Source: Own work, based on the BIGS cyber policy database. No claim to completeness. Last updated July 2017.

1.4.2 Premium Volumes

The cyber insurance market is very dynamic. If the most current figures are to be trusted, the premium volume in Germany has tripled in the last two years. For late 2015, KMPG estimated the premium volume in the cyber area at 30 million EUR[47], Erichson at 20 million EUR[48]. By early 2017, the volume estimated by KPMG for 2016 had increased to 90 to 100 million EUR[49]. Recent cyber attacks are suspected to be the cause of this increase.

For example, Munich Re subsidiary Ergo launched a cyber insurance policy targeted at small and midsized companies with revenues of up to one million EUR in October 2016. Since then, several hundred policies have already been sold. In the case of Byte Protect, an AXA product (see Table 1), demand is said to have increased by 500 percent from 2016 to 2017.[50] Some of the policies and their premium volumes listed here, as well as the current volume of the market, must therefore be considered as snapshots of the current situation.

1.4.3 Coverage

Individual coverage sums of up to 100 million EUR can be found in the stand-alone cyber insurance policies examined. This does not include individual insurance contracts between large corporations and insurers and the coverage sums negotiated as part of those contracts.[51]

In 2014, the first articles and books published on the subject of cyber insurance noted coverage amounts of up to 100 million EUR.[52] Recently, however, there appears to be movement in this area. At events and discussions held in 2016 and 2017, maximum coverage amounts of up to 350 million EUR in the German market were mentioned. In the wake of the WannaCry incident, the first policy offering coverage of 500 million EUR is under discussion by market participants.[53] However, in the German market, such sums can only be offered by an insurance consortium.[54] The foreign market in particular can provide additional capacity in this regard.[55]

For Europe, estimations are that, for the year 2016, 63 percent of companies have no cyber insurance, 25 percent have protection up to 50 million EUR and only 12 percent have obtained insurance coverage which goes beyond this level.[56]

The cost for a similar level of coverage in other areas, such as fire, is generally much lower For example, whereas a 1 million EUR of cyber insurance coverage costs between 7,000 and 15,000 EUR on the German market, five times as much coverage for other risks such as fire is available at half of the cost (4,000 to 24,000 EUR).[57]

1.5 Forecast for the Cyber Insurance Market in Germany

In the expert interviews, large corporations with revenues of more than one billion EUR were mentioned as the principal drivers behind the growing number of cyber insurance policies purchased to date. But small and medium sized enterprises (SMEs) are increasingly the focus of targeted IT attacks. For example, after an incident in a hospital in Neuss that attracted considerable media attention and that resulted in losses of around 1 million EUR[58], press reports predicted that hundreds of new policies were being purchased at the end of 2016.[59] In May 2017, the WannaCry incidents again drew increasing public attention. But apart from encryption-based ransomware, levels of IT protection remain rather weak. According to several polls, more and more managers are aware of the risk, but that does not necessarily mean that they see themselves as threatened (see also Chapter III, section 3.1).[60]

1.5.1 Market Growth among SMEs

In light of the increasing threat, the rapid expansion of stand-alone as well as integrated cyber modules would be expected. According to BITKOM, 61 percent of all cyber attacks are now being directed at SMEs.[61] According to Symantec, the share of attacks for small companies with up to 250 employees increased from 18 percent in 2011 to 43 percent in 2015.[62] Nevertheless, individually negotiated policies mainly with large companies account for the large majority of cyber insurance policies currently in effect.

Stand-alone cyber insurance or the integration of cyber insurance modules into conventional insurance contracts is the exception rather than the rule with SMEs. Major growth is expected in this area in particular, which according to the defin-

ition of the Federal Statistical Office (DESTATIS) encompasses more than 99 percent of German companies. This will have a correspondingly significant influence on the cyber insurance market.

1.5.2 All-Risk vs. Named Perils Coverage

All-risk coverage is widespread in the property insurance market. It fundamentally covers all hazards that are not explicitly excluded. To an increasing degree, however, exclusions for cyber risks are featured in the conditions of such insurance contracts. These run contrary to the all-risk concept and lead us back to named perils, namely the exclusive insurance of specified risks and their consequences.

As shown in Chapter III, Section 1.3, the cyber insurance policies on the market are mainly characterized by the enumeration of insured causes and consequences of damages and losses. Both coverage variants are conceivable as far as contemporary industrial insurance and cyber insurance as a component of industrial insurance are concerned. Here too, generally accepted procedures related to these policies have yet to coalesce.[63] This is one area where better data in the calculation of risk could bring a return to all-risk coverage in property and casualty insurance over the long term.

1.5.3 Market Outlook

In the opinion of experts, the cyber insurance market for 2015 is estimated to have a moderate premium volume of 20 to 30 million EUR[64]. For comparison, premium volume for business fire insurance is 6 billion EUR[65]. All market participants, but especially those in the insurance industry, expect strong growth in the coming years. For Europe as a whole, AGCS predicts a market with premium revenues of 700 to 900 million EUR.[66] Allianz and AXA expect a premium volume of up to 300 million EUR in 2021 in the German business insurance segment alone.[67] Including private insurance, KPMG estimates a cyber insurance premium volume in the tens of billions of EUR for 2036.[68]

Over the intermediate term (2021), KPMG calculates insurance premium volumes of between 420 and 880 million EUR for business and private insurance customers in the German speaking world. In an extreme, long-term scenario, a premium potential of up to 26 billion EUR is predicted for 2036.[69]

Because contract terms have mostly been limited to a year up to now, these statements are very uncertain and especially susceptible to short-term spikes in the issuance of new contracts. So far, past expectations of positive growth, such as those that currently exist for the future, have not come to fruition. The sporadic growth in the market is rooted in uncertainty on the supply side on the one hand, and in a lack of demand on the other (see Chapter III, Section 2).

1.5.4 Insurability of Industrial Cyber Risks and Critical Infrastructure

This study has a special focus on industrial cyber risks and especially on critical infrastructure. In brief, it can be said that industrial control systems (ICS) are insurable within the framework of industrial insurance, especially when insurance brokers are involved. But such individualized insurance solutions are usually only provided to large companies within the framework of existing relationships with insurers. Separate and reliable figures for the industrial cyber insurance market are not available.

To date, critical infrastructure and its ICS-related vulnerabilities have not been explicitly served by insurers. Loss scenarios, such as the interruption of critical infrastructure operations due to an attack on an ICS, are not addressed in the GDV model terms and conditions. But if the model terms and conditions find wide acceptance, there is at least a good chance that it will become easier for SMEs to obtain cyber insurance policies in the near future and that the premium volume for SMEs on the market will grow significantly. However, one limiting factor must be noted, namely the fact that the proposed terms and conditions are focused on data security.

2. Barriers to the Development of the Cyber Insurance Market

Based upon the above analysis of the cyber insurance market, the complexity and somewhat non-transparent nature of the general cyber insurance market in Germany is clear. Fundamentally, the analysis shows a low premium volume as well as sporadic growth in the market, which is caused by various factors on the supply and demand side. In brief, the sporadic market growth has its origins partially in a market failure, which is in turn due to information asymmetry on the demand side. Where the market for critical infrastructure providers is concerned, we can essentially speak of the market as non-existent.

In the following sections, market barriers will be presented as explanatory factors behind this situation. First, the market barriers to the development of the cyber insurance market in Germany can be divided into general barriers and barriers specifically relevant to the field of critical infrastructure. The barriers will be identified on both the supply and demand sides and will be presented separately below (see figure 7 and figure 8).

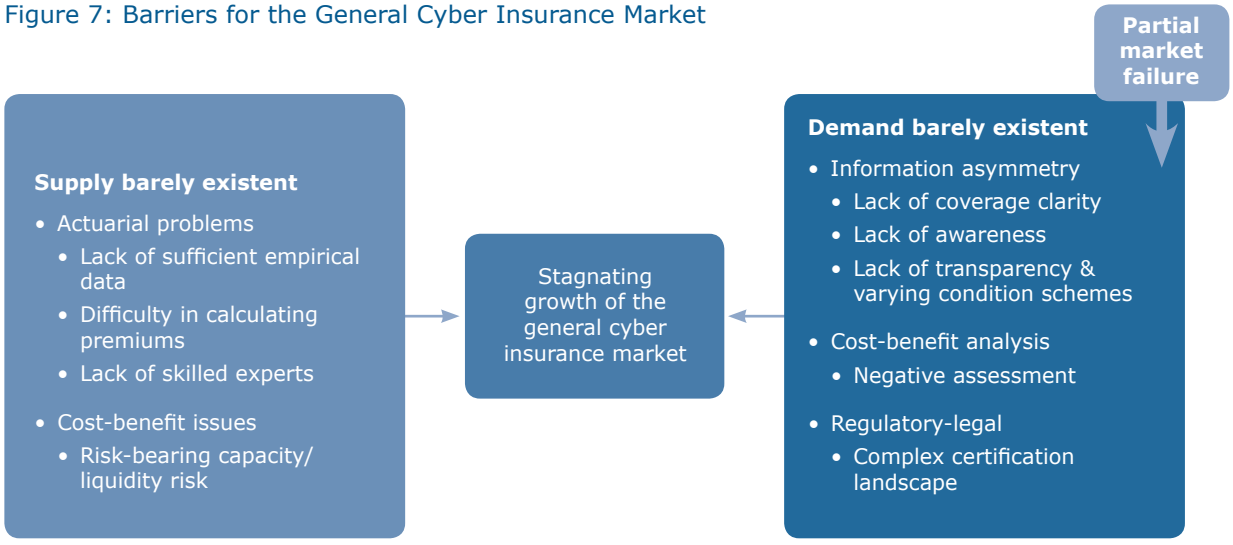
The following discussion of the market barriers is the result of an analysis of interviews conducted with key stakeholders as well as a qualitative analysis of the current practice in cyber insurance and the cyber insurance discourse in Germany. The results and the resulting categories of market barriers, as well as the typologies of suppliers and "non-demanders", are therefore purely of a qualitative nature and do not claim to be exhaustive. They should also not be understood as fixed concepts, but rather serve to illustrate the current supply and demand side barriers to tap the full potential of the cyber insurance market in Germany.

Because in the vast majority of cases obtaining a cyber insurance policy, and even more so compensation for losses that may be incurred, is tied to the fulfillment of minimum standards of IT security, questions then arise about the scope and extent of these standards and how compliance with them can be proven, for example through a certification process. For type 4, we can say that the barriers that result in the lack of demand for a cyber insurance product are based on a multitude of different and mutually dependent factors.

2.1 Barriers for the General Cyber Insurance Market

Although, as discussed above, a broad range of offerings from insurance providers is now available, this is not reflected in demand that corresponds to this supply. But the supply side itself also exhibits various factors that currently impede the comprehensive development of products on the market.

Figure 7: Barriers for the General Cyber Insurance Market



Source: Own figure.

The development of cyber insurance products opens a lucrative new market for insurance providers, but this market can also carry risks to the providers themselves. One of the central arguments that is frequently mentioned in this context is the actuarially unclear data about the frequency of losses from cyber attacks and the estimation of the scope of the losses. To date there has been very little or no experience in this area, which makes it impossible to determine the likelihood that cyber attacks will occur. This in turn makes the assessment of cyber risks more difficult – further complicated by the simultaneous lack of suitable experts on the subject – and thus also makes it hard to adequately calculate premiums.

This lack of empirical data on cyber risks and cyber losses also leads to a fundamental uncertainty about whether providing cyber insurance products will in fact be profitable for insurance providers over the long term, or whether these products possibly represent a risk to the providers themselves. In contrast to other insurance segments, the cyber field is very dynamic, new loss scenarios are very difficult to predict and their scope is difficult to define.

One problem in particular in this regard are cumulative damages. For this reason – as explained in the market description above – the insurance products have a strong focus on the so-called support services with which cyber losses and damages to a company's reputation can be reduced.

A look at the demand for cyber insurance products also supports the weak demand diagnosis; demand is currently quite far from completely exploiting the full potential of the market. The barriers on the demand side can initially be divided into three categories (see figure 7): information asymmetry, cost-benefit, and regulatory-legal. Drawing upon these demand-side barriers, we can derive four types of companies who do not demand cyber insurance, which we call "non-demanders" (see also Table 2):

- Type 1: Lack of IT risk awareness, so insurance is viewed as irrelevant.
- Type 2: Are aware of IT risk but regard existing protections as adequate.
- Type 3: Are aware of IT risk, regard existing protection as inadequate, but have a negative assessment of the cost-benefit ratio of cyber insurance.
- Type 4: Are aware of IT risk, regard their existing protection as inadequate, have a fundamentally positive assessment of the cost-benefit ratio of cyber insurance, but barriers (for example, information asymmetries) exist to purchasing a policy or no appropriate insurance solution is offered by the supply side.

As far as barriers on the demand side are concerned, first and foremost we see both a lack of individual and societal awareness at the corporate level for the topic of IT risks as well as of the realistic dangers and potential losses that may result from them, for example due to cybercrime, large scale cyber attacks, but also technical failure and human error. After all, if there is no corresponding awareness of the risks in this area, the question of whether to mitigate such risks through cyber insurance does not arise (type 1).

In the case of the next type (type 2), although a fundamental awareness of cyber risks exists, the existing level of protection is (correctly or incorrectly) regarded as sufficient. The two other demand types are characterized by an awareness of cyber risks as well as the assessment that existing protection is inadequate. But whereas type 3 negatively assesses the cost-benefit ratio of cyber insurance, for type 4 the barriers to purchasing cyber insurance lie elsewhere.

This is where aspects that are a result of information asymmetry before the conclusion of a contract between an insurer and a potential policyholder come into play. Due to the knowledge edge held by the insurance company, the prospective purchaser of the insurance is only partially able to evaluate the services provided. For example, which offer is even the right one? Is the level of coverage adequate? Which cyber risks can and should be covered by a cyber insurance policy? This question also requires the company to have previously addressed the matter of which cyber risks it actually faces. Here we run up against the same difficulties which were already described on the supplier side, in addition to the question of which of the many

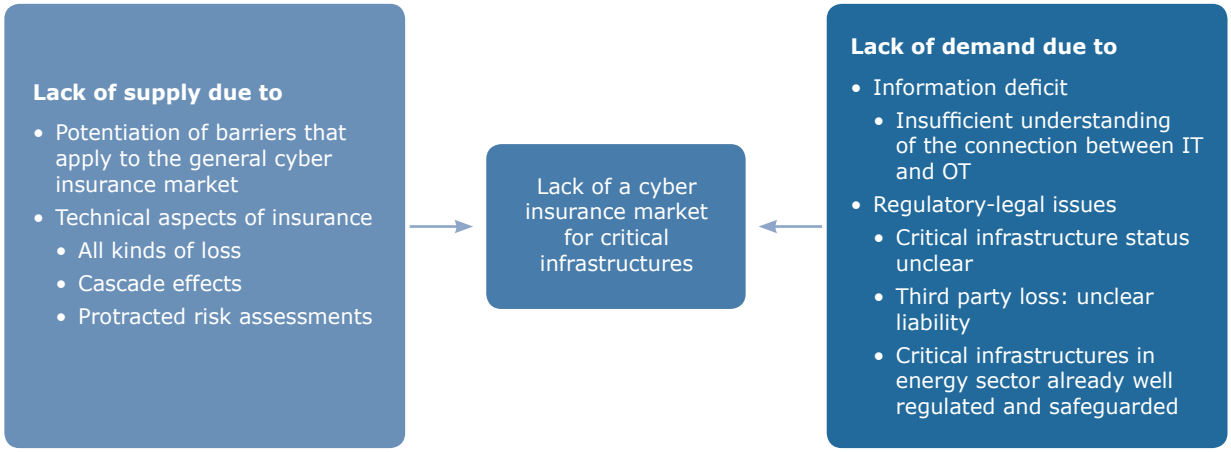
products available are appropriate to address the company's specific risks. What are the terms and conditions required to obtain a cyber insurance policy and in which cases will a given loss be covered?

Because in the vast majority of cases obtaining a cyber insurance policy, and even more so compensation for losses that may be incurred, is tied to the fulfillment of minimum standards of IT security, questions then arise about the scope and extent of these standards and how compliance with them can be proven, for example through a certification process. For type 4, we can say that the barriers that result in the lack of demand for a cyber insurance product are based on a multitude of different and mutually dependent factors.

2.2 Barriers for the CI Cyber Insurance Market

A focused look just at the cyber insurance market for CI strengthens the impression that this market can effectively be said to be non-existent. All of the market barriers identified for the general cyber insurance market are also relevant for the cyber insurance market for CI. At the same time, they are exacerbated by the criticality of the critical infrastructures and the somewhat differently structured loss potential. On the insurer side, the roots of the lack of supply are compounded by actuarial barriers related to the possible types of damage, the extent of cascade effects and risk assessment processes. These risk assessment processes are not only time consuming, but there is also a lack of trained personnel to conduct them (see figure 8).

Figure 8: Barriers for the CI Cyber Insurance Market



Source: Own figure.

A look at the cyber insurance discussion in Germany provides some initial explanations for the non-existence of the market: to date relatively few actors have addressed the matter of the insurability of IT risks for CI and standardized offers for CI are not available. This especially applies on the part of the insurance industry, and can be illustrated by the model terms introduced by the German Insurance Association (GDV) in April 2017.[70] For the insurance industry, these model terms have a special, functional quality because they represent a kind of blueprint for a standardized cyber insurance product. However, they do not yet address the issue of products especially for CI. At the same time, it must be noted that the IT Security Act was still in the process of implementation during the time when the GDV model terms were being developed (2015 to 2017). Overall, the IT Security Act can be seen as a driving factor for the CI cyber insurance market (also see Chapter III, Section 3.2), but the implementation phase has initially created uncertainty about which operators in each of the CI sectors will actually be classified as critical.

In a simplified form, the debate on the supply side can be reduced to two opposing positions: the position that cyber risks for CI are insurable versus the position that they are not insurable.

Thus, the debate about the insurability of critical infrastructure IT risks is reminiscent of the debate about the insurability of nuclear power plants.[71] For a long time, the core of this debate was also shaped by two opposing positions: either nuclear power plants are insurable, or they are not. In that instance, the great fear was that the damage caused by a nuclear accident could exceed the financial capacity of the insurers. However, to determine whether this is the case, the total extent of the damage caused by a reactor accident must first be clarified. At the time, this question was also very controversial.[72]

A similarly unclear scenario applies to critical infrastructures. What kinds of major disasters can really be caused by CI cyber incidents? Different scenarios are conceivable in each of the different CI sectors. What are they and how high would the potential for loss be in each case? What would happen if cyber attacks not only lead to property damage, but also to casualties, something that has so far not been addressed by cyber insurance? These questions have yet to be answered, especially for critical infrastructures.

The non-insurable position is thus based in the uncertainty of the threat posed by cyber risks to CI, the potential extent of the losses involved – especially cascade effects – and consequently the possibility that coverage amounts may not be sufficient. If you take a closer look at the coverage available in the German market – currently up to 100 million EUR – this uncertainty is not unjustified.

The reasons for the lack of demand can be classified into two categories: information deficit and regulatory-legal aspects. From these we can then derive essentially the same types of non-demanders as in the case of the general cyber insurance market, albeit if the causes for them differ somewhat. Thus, for example, for type 1 non-demanders, one component of the lack of awareness of IT risks is a lack of awareness of the vulnerability of networked industrial control systems. For type 2 non-demanders, the assumption that existing protections are adequate may be due to the fact that CI sectors, such as the energy sector, are already highly regulated. However, beyond these four types, there is a fifth type, for which a new aspect plays a central role: the question of liability (see Table 2).

Table 2: Types of Non-Demanders in the Cyber Insurance Market – in General and for CI

	General Cyber Insurance Market	Critical Infrastructure Cyber Insurance Market
Non-demander type 1	Lack of IT risk awareness, so insurance is viewed as irrelevant.	
Non-demander type 2	Are aware of IT risk, but regard existing protections as adequate.	
Non-demander type 3	Are aware of IT risk, regard existing protection as inadequate, but view a cyber insurance as cost-ineffective.	
Non-demander type 4	Are aware of IT risk, regard their existing protection as inadequate, view a cyber insurance in principle as cost-effective, but barriers exist to purchasing a policy or no appropriate insurance solution is offered by the supply side.	
Non-demander type 5		Are aware of IT risk, regard their existing protection as inadequate, but liability is unclear or they rely on force majeure exemptions or coverage by the state.

Source: Own figure.

Although these barriers at first might suggest a rather sober analysis of the situation of the cyber insurance market in Germany in general as well as for CI, it is still possible that the insurance market could change in the future and develop favorably with the appropriate incentives. This possibility will be examined more closely in the following section. As far as a cyber insurance market specifically for CI is concerned, the question of the liability of CI operators and state intervention will determine the future of this special market.

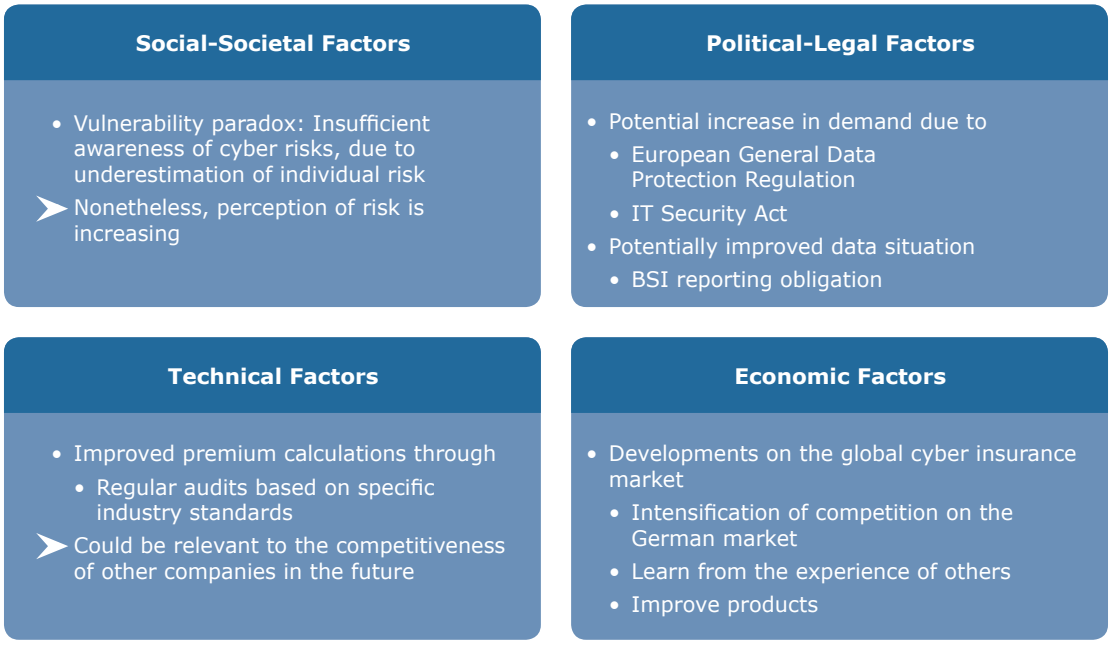
3. Positive Factors Influencing the Development of the Cyber Insurance Market

Building upon the market barriers identified above, the following section shall analyze – for Germany – factors that could positively affect the development of the cyber insurance market. In the case of the factors that are investigated as having a positive influence on the market, we loosely base our approach on a STEP analysis.[73] This means that we will first examine social-societal and political-legal factors and then technical and economic factors. In this analysis, the central factors that can credited with exerting a positive influence on the further development of the cyber insurance market will be identified and described. Along with the influential factors that can be found at the political-legal, technical and economic level, social and societal factors build the framework within which all of the other factors are able to exert influence.

3.1 Social and Societal Factors

One of the greatest market barriers for the cyber insurance market is the lack of awareness of cyber risk. There are a variety of aspects to this lack of awareness, starting with the fact that there is a fundamentally insufficient understanding of the risks connected to cyberspace and going on to a failure to recognize the necessity of addressing the security of IT infrastructures. For the subject of this study, namely safeguarding against cyber risks by obtaining cyber insurance, this means that the demand for cyber insurance can only be based upon a fundamental sensitization for the topic of cyber security and a strong awareness of the real cyber risks that companies are facing.

Figure 9: Factors Influencing the Cyber Insurance Market in Germany



Source: Own figure.

In Germany, for the first time, awareness of cyber risks on the part of companies has increased significantly in the last few years. Thus, for example, the Allianz Risk Barometer named cyber risk the greatest risk for businesses in 2016.[74] However, a FORSA poll of SMEs with up to 50 million EUR in revenues that was commissioned by the GDV revealed that, although up to 75 respondents acknowledged the high level of cyber risk for SMEs in Germany in general, 63 percent estimated their own individual risk to be low.[75] Whereas the Allianz Risk Barometer bases its results on surveys of experts, the FORSA poll also asks respondents about their individual risk perceptions. The discrepancy is clear: although there is a strong awareness among policymakers and experts of the cyber risks as well as a general awareness of the threat posed by cyber attacks, at the individual level there is an assumption that these threats affect someone else, not the individual themselves.

It is possible to draw an analogy between the individual perception of cyber risks and emergency and disaster preparation. In Germany, the so-called vulnerability paradox is often referred to in the context of societal awareness of risk where large-scale emergencies in catastrophe and crisis situations are concerned. The BMI's national strategy for the protection of critical infrastructure states that:

The „[...] fact that increasing robustness and lower susceptibility to failure lead to the development of a misleading sense of security, and that the effects of a failure that may occur despite them are disproportionally high, is called the vulnerability paradox"[76].

It can be confirmed that a similar situation currently exists in regard to the awareness of cyber risks, especially as cyber risks and the damage associated with them are to some degree too abstract for the individual to generate a feeling of concern. Nevertheless, we can expect that the awareness of the risks emanating from cyberspace will continue to increase. This is because an awareness of risk can develop in response to events, for example through the direct or indirect experience of cyber attacks. More incidents lead to an increasing threat scenario and thereby generally to an increased awareness of and sensitization to risk.

Overall, the general awareness of cyber risks by society as a whole is increasing. At the same time, increased reporting on the subject of cyber insurance is also noticeable, so that the issue of the insurability of cyber risks is also attracting attention outside of specialist circles.

From a social-societal perspective, there are good reasons to believe that the cyber insurance market in general will grow in response to certain incidents. If we turn to the development of the insurance market specifically for critical infrastructures, the increased threat scenario has not yet resulted in a specific boost for this special market. Rather it is policymakers and political-legal factors that will play a central role in its future development.

3.2 Political-Legal Factors

The political sphere in Germany can presently be characterized as having a strong focus on the topic of cyber security, one that cuts across ministerial and departmental boundaries. The list of strategies, initiatives, newly created institutions, and so on is long. All of the institutions concerned with cyber security are also strongly increasing staff levels.

In the following section, two important legislative developments will be highlighted as political and legal factors that could have a positive effect on the cyber insurance market in Germany. High hopes are for the future development of the cyber insurance market are tied to these two pieces of legislation:

1. The European General Data Protection Regulation (GDPR) as well as the
2. The IT Security Act (IT-Sicherheitsgesetz), which is considered to be the national law implementing the Directive on Security of Network and Information Systems (NIS Directive).

As explained in Chapter II of this study, a distinction can be made between cyber security in IT and OT. Keeping the German cyber insurance market in mind, these two legislative pillars must be weighted differently. The implementation of the GDPR in national legislation could have more of an influence on aspects connected to office IT. In contrast, the IT Security Act – depending on the

sector in question – could have more overarching influence on both areas.

The European Data Protection Regulation could be a central new factor influencing the development of the German cyber insurance market. Expectations are that the new regulation will result in a heightened sensitivity for the subject of data-related IT security at private businesses. For example, following the implementation of the GDPR, penalties for violations of the law of either 20 million Euros or four percent of the violator's annual revenues are possible.[77]

However, these legal changes tied to the European General Data Protection Regulation as well as the expectations of potential changes in the cyber insurance market are primarily only connected to data protection aspects of IT security and are therefore unlikely to have major influence on industrial IT security. It is also unclear whether it would be possible for cyber insurance to pay for any of the corresponding fines.

The hopes that the GDPR will have a positive influence on the cyber insurance market are essentially based on a comparison with the market developments in the USA. There, the much more rapid growth (compared to Germany) in the cyber insurance market, which has existed since the 1990s, is held to be a result of high punitive damages awarded by the courts. These have led to a stronger demand for cyber insurance products.[78]

However, an examination of the GDPR alone is not sufficient to achieve the aim of this study, namely to investigate the market and the development potential for cyber insurance in industry and critical infrastructure. Much more important are the aims of the security policy in the field of IT security as it relates to critical infrastructures – and therefore the IT Security Act passed in 2015. The act is exclusively directed at the operators of critical infrastructures and also pertains to the interfaces between industry and ICS and CI, for example in the energy sector.

The IT Security Act, passed in 2015, is an important legislative milestone for IT security in Germany. The act was accompanied by two subsequent regulations that are incrementally directed at critical infrastructure operators:

Figure 10: The Classification of Critical Infrastructures in Germany

Source: Own figure based on the IT Security Act.

The most important legislative changes associated with the IT Security Act include:

1. The definition and identification of CI operators in the sectors addressed by the law;
2. The cooperative development of sector-specific IT security standards ("Stand der Technik" – "state of the art") in the individual sectors and the review of these standards by the BSI;
3. Mandatory implementation of the industry standards ("state of the art") by CI operators and the obligation to prove their compliance every two years, in the form of audits and certifications;
4. The establishment of a point of contact for the BSI in individual companies; and
5. The introduction of a requirement to notify the BSI in the event of "significant disruption" of IT security.

Specific consequences for the cyber insurance market can be deduced from the legislative changes mentioned above. Point 1 legally

defines the critical utility services provided by a CI company. So-called support services, specific forensic services, can be used to contain the extent of potential or successful cyber attacks. The implementation of industry standards associated with points 2 and 3 ("state of the art") and the notification requirement can also be assessed as factors that will influence the cyber insurance market. Thus, for example, the notification requirement can contribute to an improvement in the data situation about cyber incidents in Germany, as long as the data are provided to the insurance industry in anonymized form.

The IT Security Act does not directly address the liability of CI operators as far as cyber incidents are concerned. However, this is indirectly addressed by the introduction of sector-specific minimum standards. This is because a central criterion in determining liability is whether a given action was willful or negligent. If it can be proven, however, that minimum standards were fulfilled, providing willful or negligent action becomes more difficult. In this instance, it could be important to safeguard against compensation claims from third parties by obtaining cyber insurance. However, the fact that insurance could have a negative effect on risky behavior could also be problematic, as long as the insurance does not specify conditions that contradict these.

In a broader sense, in addition to the GDPR and the IT Security Act, the model terms published by the GDV also hold special relevance for the development of the cyber insurance market. With their publication, a quasi-standard was set for cyber insurance in two ways. First of all, they lay an important foundation for the definition and delineation of cyber insurance. Second, with their risk assessment conditions, they provide quasi-standards in regard to IT security and thereby fill gaps left by the GDPR and the IT Security Act. While the model terms do not yet refer to CI, with the implementation of the IT Security Act, the general question of the insurability of CI cyber incidents is likely to be raised again.

3.3 Technical Factors

This section is not intended to provide an overview of technical advances related to IT security, but rather to address the significance of the term "Stand der Technik" – English "state of the art" – as a positive factor.

The term was frequently criticized in the course of the passage of the IT Security Act because it was unclear what it exactly meant. However, as a legal term, it takes into account the fact that the technical environment and technical developments are always more dynamic and changing faster than legislation. The "state of the art", or better put the "state of IT security," will especially influence the criteria for the insurability of companies in the CI sectors, assuming that a minimum standard of IT security is seen as a prerequisite for obtaining insurance.

As has already been outlined above, the IT Security Act and its associated sector-specific regulations require CI operators in water, energy, food, information technology and telecommunications (round 1) and transportation and logistics, insurance and finance, and health (round II) to implement sector-specific IT standards ("state of the art"). These standards are cooperatively developed within the given sector and then reviewed by the BSI. The CI operators regulated by the IT Security Act are also required to regularly subject themselves to audits on the implementation of these minimum standards. Here the aspiration is to particularly influence the level of IT security at CI operators, whose IT security standards were not especially high before the IT Security Act entered into force, and more broadly to equalize the level of IT security in all sectors specified in the law. On the one hand, the requirement to implement the industry-specific minimum standards means that operators must confront the topic of IT security, as they are legally obligated to implement the standards. On the other hand, for CI operators, the requirement may again raise the question of whether to protect themselves against cyber risks with cyber insurance. In addition, for the insurance companies, the introduction and regular auditing of IT security standards is likely to support attempts to examine the insurability of the companies in question and to conduct risk assessments within the framework of underwriting services.

Consequently, the sector-specific minimum standards can be assessed as positive factors influencing the CI cyber insurance market in two ways. At the same time, the IT standards in the

respective sectors could also become prevalent in companies that are not subject to regulation by the IT Security Act. Court decisions in future damage cases will be a driving factor in this regard. The state of the art in the industry could also be a decisive factor, even though it is not legally binding for the company. To remain competitive in the future, it could also be necessary for other companies in the CI sectors to also implement those sectors' state of the art IT security standards. Therefore, long-term exchange and cooperation with technology providers in this area will be important.

3.4 Economic Factors

In regard to the economic factors that could have a positive influence on the further development of the cyber insurance market, it is worth taking a look at the international dimensions of cyber insurance. As initially described in the section of this paper addressing the market (see Chapter III, Section 1), the German market is dominated by international providers. Due to the predicted growth for Germany, it is to be expected that more insurance providers will enter the German market, resulting in increased competition.

Presumably, the insurance companies would then be competing with providers who have more experience[79] in cyber insurance and could also provide higher coverage.[80] The domestic insurers could use this knowledge held by international insurance actors, combining it with their historically based market-specific knowledge of Germany. They could then apply the result to pursue a follower strategy and make use of home field advantage to further refine their own products.

IV CONCLUSIONS ON THE CYBER INSURANCE MARKET IN GERMANY

1. Conclusions

The above results show that the cyber insurance market in Germany can, for the most part, be assessed as a market with strong growth potential. This is clear in light of our analysis, especially from the perspective of insurance and reinsurance companies as well as insurance brokers. However, a closer look at the spectrum of theoretically insurable IT risks – from a data breach to a black out due to a cyber attack – shows that Germany does not have a cyber insurance market that functions at a level needed to sufficiently cover these risks, and that the insurability of certain large scale CI failures is regularly called into question. To date, demand by CI operators barely exists, also because of a lack of supply. Demand for a general cyber insurance market is also currently sluggish.

In regard to the general – not CI-related – cyber insurance market, it can be assumed that the growth of this new market can be increased with the properly applied adjustments. This process may therefore have to be regulated by lawmakers via the appropriate policy framework – like in the case of the IT Security Act – or stimulated by the state or insurance companies using appropriate incentives.

IT security is a challenge that must be addressed by all of society. The appropriate protection in the form of hardware, software and services cannot and must not be provided by the state alone. The protection of its citizens from external threats (such as cyber attacks) and internal threats (such as crime) is a central task of the state. That does not mean that private actors need not contribute to this effort.

Protection against burglary represents a useful analogy in this regard: although the state uses the police and the justice system to implement

preventative and suppressive measures that reduce the threat posed by burglars, residents should still lock the entrances to their homes. Typically, they are even required to do so to fulfill due diligence requirements listed in their renter's or homeowner's insurance. The situation is similar in regard to IT security. When measures that reduce the IT risks for businesses are created, provided and financed, the question is consequently raised of who bears responsibility – the state or private business. Ultimately, it is normally the companies themselves – regardless of state measures that are often superordinate, overarching and generally preventative in nature – that must be held to account.

Against this background, the insurance industry can be an important driver, if it cushions the damage potential to businesses connected with cyber risks on the one hand by offering cyber insurance policies, while on the other hand tying the underwriting of these policies to appropriate security standards. Only when both of these factors coincide can we assume that the level of IT security in Germany at insured businesses will increase. This is because cyber insurance will not only exert reactive influence, but at the same time also preventative influence, enabling the insurance industry to play a central role as an important actor in the IT security landscape in Germany.

Despite the increased awareness of cyber risks on the part of businesses, continuing to increase the visibility of cyber security as a central aspect of business security is paramount to the further development of the cyber insurance market in Germany. Policymakers, private industry and the academic community are equally called upon to take action. As long as businesses continue to consider risks as not really being relevant to them, all ambitions in this area will come to naught. The next step is closely connected with this, namely appropriate arguments to corporate management by those responsible for IT security that expenditures for IT security, including cyber insurance policies, are necessary and pay for themselves. A critical future step in this regard could be the question of the liability of company management for first and third party damages resulting from cyber attacks; this will be dependent on the first court rulings in such cases. If company management is ruled to be responsible for averting all possible threats – as is the case under the German Stock Corporation Act (Aktiengesetz) – this would also include cyber risks. This means that corporate management can be made personally liable if it does not take sufficient care to protect the company from such risks.

However, the positive influence of cyber insurance and subsequently of the insurance industry on the IT security of companies and the manufacturing industry in Germany, which is at the focus of this paper, is only possible to the extent that a company can estimate damage from a cyber attack in monetary terms. Cyber insurance therefore only serves as a means of risk transfer when the damages that are caused by a cyber attack can be quantified in financial terms.

A central criterion for whether cyber insurance can be a suitable instrument for risk transfer as well as an instrument for improving the IT security level at businesses is the requirement that a loss has to be capable of being expressed in monetary terms, within reasonable limits, and that insurance companies are capable of bearing the loss.

This would seem to be a challenge in the dynamic field of cyber threats, but not one that is insurmountable. In many ways, clarity can be provided if a company looks at other relevant potential risks for itself – for example, an interruption of operations, sabotage, espionage, data theft, etc. – and takes cyber attacks into account as one additional cause of damage. After all, digitalization initially changes the cause of damage to a company, but not necessarily the damage itself.

However, if we take the broader societal function of CI as a basis and consider risk scenarios under which the damage to society would be so high that – from an ethical and moral perspective – money is no longer an adequate means of compensation, everything must be done to prevent such damage. Depending on the criticality of the CI or industry in question, cyber insurance is not the appropriate means to transfer risk and create positive incentives to improve the level of IT security.

The insurability of cyber risks in the case of critical infrastructure and industrial companies therefore depends on their respective criticality and the damage potential associated with cyber attacks.

This means that, when a high degree of criticality and corresponding damage potential due to cyber attacks is involved, the state must impose security requirements for IT in these areas, like the requirements that are already the case in the energy sector, a highly regulated CI sector. The high security requirements imposed by the state could then be accompanied by a state guarantee which would relieve CI operators of liability in a worst case scenario. Thinkable in this case would be a kind of "cyberpool," similar to the insurance pool established for operators of nuclear power plants, which would reinsure primary insurers in the event of large-scale catastrophes.[81]

Here, however, we must return to the aspect mentioned previously, namely awareness of IT security and cyber risks. This is an extremely complex field characterized by the entanglement of office IT, production IT, CI and crisis and catastrophe scenarios that could be unleashed by cyber attacks. Attempts to reduce this complexity by dismissing such scenarios, for example worst case cyber-catastrophes, as completely unrealistic are not helpful, nor is it productive to popularize doomsday scenarios. Instead, what is necessary is a realistic assessment of the threat situation. Towards this end, scenarios for damage to specific CI sectors that could actually be caused by a cyber attack must be developed, categorized according to the extent of the resulting damage, and converted into a monetary figure. On this basis, it would be possible to reconsider the limits to insurability, a topic which is currently under debate for CI.

2. Recommendations

The study has shown that the cyber insurance market in Germany is a market with strong potential for growth. However, adjustments must be made in several areas so that cyber insurance can establish itself as an integral component of IT risk management and the cyber insurance market can develop further. To complement the factors that positively influence the development of the German cyber insurance market examined in Chapter III, Section 3, the following recommendations for the state, insurance industry and private companies are made. However, these recommendations are accompanied by the qualifier that, due to the lack of a cyber insurance market for CI, they are made for the general cyber insurance market. At the same time, in many respects these recommendations are also applicable to CI.

2.1 Recommendations for the State

• Reduce information deficits through mandatory notification requirements

Insufficient information about cyber risks makes the reliable calculation of premiums for cyber insurance much more difficult. The most advanced market in this respect is the market for cyber insurance for data breaches in the United States.[82] There, the advances in the market were accompanied by the successive expansion of requirements to notify affected customers. This development began in 2002 with a change in state law in California. In the meanwhile, a notification requirement now exists in 48 states, and notification requirements have been put in place by federal law in some industries. In most cases, so many customer data are affected by a hacker attack that the obligation to notify all affected customers de facto amounts to a disclosure obligation. The data collected in this way can be used by insurers to better calculate their premiums and offer attractive cyber insurance policies that are in demand.

In Germany, notification requirements were first introduced with the IT Security Act in 2015, and only for companies in CI. We must therefore first wait and see if this change in the law results in an improvement in the information situation, resulting in an optimization of the products available on the cyber insurance market. However, this requires the information to be provided to insurers in anonymized form. If there is no improvement, the possibility exists of expanding the notification

requirements following the US example and improving enforcement of the notification requirements.

• ***Reduce information asymmetries with insurance standards and databases***

For potential customers, the insurance market is very confusing because no uniform standards have been established, which makes it difficult to compare different insurance products. The solution to this problem is primarily the responsibility of market players. In 2017, the German Insurance Association (GDV) took an important step in this direction by publishing its model conditions for cyber insurance. Nonetheless, if information asymmetries continue, state support for additional steps would be worth considering. The United Kingdom can serve as an example in this respect. The British government, working together with insurers, has published guidelines for cyber insurance and also included the databank of the British Insurance Brokers' Association (BIBA) in this effort (see also recommendations for the insurance industry).[83]

• **From a transfer of risk to the reduction of risk through security standards**

The function of insurance is to transfer risk, but it can also contribute to risk reduction if observing security standards is either a condition for obtaining an insurance policy, or at least is promoted through reduced premiums. To date, however, the cyber insurance market has primarily been focused on risk transfer; the potential for risk reduction is not being exploited. In the US, a market for cyber insurance has established itself in which a risk assessment is conducted, but in which the observance of security standards barely plays a role.[84] In the UK, an attempt was made to promote the observance of state-supported standards, the Cyber Essentials, through lower premiums. This, however, has resulted in higher costs of certification than the premium savings.[85] If it also proves impossible to close this cost gap in Germany, this would be an area where the state could intervene to promote the security interests of society as a whole. Increasing IT security in a specific company is not only advantageous for that specific company, but also increases overall security in a networked society. These positive externalities could justify state subsidies for security certifications or cyber insurance which would require a security certification.

• ***The state as a reinsurer in cases in which the real target is the state (terrorism)***

When issuing a cyber insurance policy, insurers conduct a risk assessment of the potential policyholder. However, some risks are not individual risks, but must be viewed as risks to entire societies. For example, cyberterrorists may attack individual companies even though their real target is the state or an entire society. It is therefore necessary and in the interests of society as a whole that such risks are not excluded from being transferred. The British insurance pool Pool Re, which underwrites terrorism risks with the support of the British government, could serve as an example in this regard. It is expected that this British insurance pool will provide coverage for cyber terrorism.[86] Such an arrangement could also be a model for Germany.

2.2 Recommendations for the Insurance Industry

• ***Comprehensive IT security assessments and premiums tied to the level of IT security***

The issuance of a cyber insurance policy may have the result that the transfer of risk to an insurance company gives the policyholder no incentives to invest in their own cyber security. This effect can be observed on the US market, for example.[87] A comprehensive assessment of the state of IT security by the insurer before the policy is issued, as well as the regular review of the level of protection throughout the term of the policy, would therefore be beneficial. This would offer the possibility to reduce the insurer's information disadvantage after the issuance of the policy and at the same time would create an incentive for the policyholder to continually improve its own level of IT security. This last aspect would also have positive effects for the society as a whole.

Differential pricing is one measure that can be taken to avoid adverse selection. Adverse se-

lection can here be described as the situation in which companies that hold cyber insurance make inadequate and lax investments in their own protection. Proven (certified) IT security measures could lead to a reduction in the price of a cyber insurance policy. This approach was taken in the UK. However, in that situation the costs of an IT security certification were too high compared to the price reduction.[88] As a result, here too, insufficient investment in IT security has been observed.

Due to the positive external effects that are associated with a proven increase in the level of IT security, but that cannot be completely redeemed by reductions in the price of policies, state support in this area could be indicated (see also recommendations for the state).

As a result, if the insurance industry, through its range of cyber policies, is not only able to transfer risk but also to increase the level of IT security among policyholders, the industry can become a significant actor in the field of cyber security.

- ***Support services***

In addition to influencing "security hygiene", the insurance industry can also position itself as an important actor in the German IT security landscape by providing support services. Support services can make it possible to mitigate and contain acute and long-term loss scenarios. This can be accomplished preventatively through loss prevention measures and reactively through a 24-hour, 7 days a week hotline, forensic services and support with crisis management and crisis communication.

Cooperation between IT security experts and insurers, such as that already practiced by IBM and Swiss Re, would be especially advantageous where forensic services and an emergency hotline are concerned. In the US, experience has shown that ex-post communications efforts after a data privacy breach, as well as the time required to identify the attack and close the breach, has an effect on the financial cost of a cyber attack.[89] In addition, for insurers this offers the opportunity to improve their knowledge base by collecting qualitative data about the types of attacks and effective reactive and preventative measures.

- ***Signaling measures to reduce information asymmetries***

In addition to the GDV model conditions, additional signaling measures should be taken to promote the reduction of information deficits on the side of policyholders. To provide truly transparent information, the necessary approach would be a portal comparing the various cyber insurance policies available on the market. Insurance companies that provide appropriately detailed information about their insurance solutions to this information platform should receive the opportunity to display a transparency seal of approval, enabling them to use the economic benefits of trust to their advantage. If a neutral party cannot be found to design and operate such a comparison portal on the open market, initial start-up funding by the state could be considered (see also recommendations for the state).

- ***Recapture German market share***

As predicted in the economic factors influencing the cyber insurance market, due to the expected growth in the German cyber insurance market, increased numbers of international insurance providers will enter this market. These providers bring several years of experience, enabling them to better address special kinds of risks. However, they lack knowledge about the market's country-specific features. German insurers should use the new international knowledge available to them, combine it with the knowledge resulting from their specific market experience, and use this to refine the competition's products to make them more appropriate for the German market. Through such a strategy, market share could be regained by a targeted appeal to domestic demand. Business interruption modules and support services should be at the focus of efforts to acquire market share in the German market and better position themselves on the global cyber insurance market. So far, these modules have not been emphasized by international insurance providers, due to the focus on data breaches.

2.3 Recommendations for Companies

• Strengthen awareness of cyber risks

A lack of awareness of cyber risks has proven to be one of the most decisive market barriers faced by cyber insurance. Aside from the fact that fundamentally all employees of a company should be sensitized to the threat that cyber risks pose, it is essential that the corporate management of a company deals with the cyber risks to which the company is potentially exposed. An IT risk management system could achieve much in this regard, but active exchange of information of an institutional nature, such as in the Alliance for Cyber Security[90], can also improve risk awareness. A variety of references for IT risk management exist in the form of different standards and guidelines for the management of information security – from DIN ISO/IEC 27001 to VdS 3473, especially for SMEs. Thus, not every company needs to necessarily launch a certification process. These norms and standards can initially serve as orientation aids. In any event, it is important that regular security audits of the company's information security management system (ISMS), established on the basis of these guidelines, are conducted.

• Reducing complexity when considering potential damages from cyber risks

In additional to enormous opportunities, digitalization also brings new risks, many of which are not yet foreseeable. However, companies must address these risks now and push ahead with efforts to minimize potential damages within the context of a risk management approach. Cyber issues will not always be the cause of direct damages. However, they can be additional variables that increase the likelihood that damages will be incurred, meaning that they can be the direct as well as indirect cause of damages.

Not only the management of IT risks in general, but also the insurability of cyber risks can be improved by precisely considering the potential damages that could result from cyber incidents, thereby reducing complex circumstances to their most important aspects. In general, digitalization tends to change the cause of losses rather than the actual loss scenario itself. For the purpose of general corporate risk management, managers must therefore know which damage scenarios are relevant for their company. These could include business interruption, sabotage and property damage, loss of customer data and destruction or theft of company data. In these cases, the cyber factor must be taken into account as a potential cause of such damages.

• Cyber insurance as a complement to IT risk management

The risks that accompany digitalization and that will confront companies today and in the future, must be addressed with the help of a comprehensive IT risk management approach. Cyber insurance can play an important role in this by transferring remaining financial risk to an insurer in the event of a cyber-incident that results in a loss. In addition, in the event of a loss, companies – especially those who do not have their own IT department – could draw upon support services offered in their cyber policies, which include forensic services and reputation management, for example.

If the insurer ties cyber insurance to the right conditions, the insurance can not only have a reactive security function, but it also can influence preventive technical and management-related IT security strategies. This is possible through the necessary adherence to and orientation to IT security standards.

For decision-makers, the growing number of cyber attacks increasingly raises the question of when cyber insurance makes sense. This study does not claim to provide an all-encompassing answer to that question. In some cases, when relatively low loss amounts are expected, it may be enough to protect oneself by setting aside enough capital and investing in IT security. In contrast, when potential damages are relatively high, insurance makes sense even despite significant investments in IT security. As a matter of principle, investments for cyber insurance must not be seen in opposition to investments in IT security. Cyber insurance cannot be a substitute for investments in IT security measures.

3. Collective Learning

In addition to the recommendations for action explained above, this study also identified another point that can be best expressed by the term "collective learning". The development of an awareness of IT risks is a collective learning process that is closely tied to the risk perceived by the individual as well as society as a whole.

As outlined in this study, regulatory mechanisms for Germany (the IT Security Act) have proven to be a trigger that, over the long term, can lead to the insurability of IT risks for CI operators and thereby for the industry as a whole. On the one hand, the IT Security Act makes it possible to collect data across sectors. However, these should also be provided to insurance companies in anonymized form. At the same time, it promotes a sustainable exchange between the relevant actors by requiring the development and implementation of sector-specific standards ("state of the art") and the explicit involvement of companies in their design. In the end, the establishment of sector-specific critical infrastructure IT standards not only leads to improved certifiability, and a common, industry specific understanding of "state of the art," but also to improved insurability on the basis of overall improvements in the ability to conduct risk assessments on the part of insurance companies and brokers.

In this way a process of collective learning can be initiated in which companies as well as public authorities, industry associations and the insurance industry participate. The long-lasting knowledge gained through such a process must be further refined and developed. Together with the IT security practices in the CI sectors, it will lead to a reconsideration of the insurability of industrial control systems and especially of critical infrastructure operators.

For security research, the insurability of cyber-risks remains a rewarding field of research, even more so when academic efforts can be based on better data. We hope that we have made a contribution to this effort.

ENDNOTES

1. Allianz (2017).
2. Allianz (2013).
3. Bundeskriminalamt (2015), p. 5.
4. KPMG (2015)(2).
5. Bundesamt für Sicherheit in der Informationstechnik (2014)(2), p. 1.
6. Bundesministerium des Innern (2009), p. 3.
7. Bundesamt für Sicherheit in der Informationstechnik (2016).
8. BIGS (2017), p. 47ff.
9. Bundesamt für Sicherheit in der Informationstechnik (n.d.).
10. Andelfinger, V. & Hänisch, T. (2017), p. 93.
11. Ibid.
12. Ibid.
13. Brück, T., de Groot, O. J. & Ferguson, N. (2014). See also Stuchtey, T. H. & Skrzypietz, T. (2014).
14. See also Baban, C. P. & Stuchtey, T. H. (2014).
15. For one example of how to approach this topic, see Bitkom (2016).
16. Prokein, O. (2008), p. 5.
17. BIGS (2017), p. 47ff.
18. See also Heidemann, J. & Flagmeier, W. (2014), p. 45 and Betterley, R. S. et al. (2017), p. 5.
19. GDV (n.d.)(1).
20. For predictions about the cyber insurance market for individuals, see for example KPMG (2017).
21. Choudry, U. (2014), p. 29.
22. GDV (n.d.)(2).
23. A more precise differentiation between the service industry, skilled trades and manufacturing and their specific risks (depending on the field of business of the respective company) will not be conducted.
24. This calculation is based on an estimate of the volume of cyber insurance premiums for early 2017 of 900 million EUR and Scenario 3 in KPMG (2017), together with the assumption that the premium volume in the property and casualty area alone is 98.4 billion EUR (excluding cyber insurance) and will grow by an average of two percent annually from 2015.
25. See also Choudry, U. (2014), p. 27ff.
26. BIGS (2017), p. 53ff.
27. Brinkmann, T. (1993), p. 72ff.
28. Bundesamt für Sicherheit in der Informationstechnik (2014)(1), p. 31.
29. This overview represents the state of the BIGS cyber security policy survey, with 24 more precisely specified policies, as of the end of February 2017.
30. McAfee (2015), p. 5.
31. See Ponemon Institute (2017)(1) for more on direct costs.
32. Ponemon Institute (2017)(2), p. 4 and Ponemon Institute (2016), p. 2.
33. Article 83 Paragraphs 4 and 5 of the GDPR.
34. One the other hand, a breakdown of US empirical data on data breach incidents shows that legally mandated fines have only accounted for five percent of the total costs in loss incidents (Netdiligence (2016), p. 7).
35. See also GDV (2017)(1) and GDV (2017)(2).
36. Insurance Information Institute (2015).
37. Choudry, U. (2014), p. 2. This situation has barely changed since 2014.
38. Ibid.
39. German insurance regulators, as part of the German Federal Financial Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht - BaFin), require that insurers clearly delineate their individual insurance classes, legally and economically. For the number of insurers in 2015, see Choudry, U. (2014), p. 1, in 2016 see GDV (n.d.)(3).
40. See also the BIGS cyber policy database.
41. About five to six insurers are new entrants on this market.
42. ACE purchased Chubb in early 2016 and the combined company is known as Chubb Limited (Naidu, R. & Das, A., 2015), ACE and Chubb policies see Chubb Limited.
43. AGCS is the industrial insurance area of the Allianz Group.
44. See also note about ACE above.
45. ERGO is a subsidiary of Munich Re.
46. Kiln Europe is a subsidiary of Tokio Marine Kiln Insurance.
47. KPMG (2017), p. 28.
48. Erichson, S. (2016).
49. KPMG (2017), p. 31.
50. Fromme, H. (2017).
51. See also Kamp, M.,Dämon, K. & Kuhn, T. (2017).
52. Heidemann, J. & Flagmeier, W. (2014) and Choudry, U. (2014).
53. Fromme, H. (2017).
54. Interview with insurance industry representative.
55. BIGS (2017), p. 53ff.
56. FERMA (2016), p. 15.
57. List, T. (2015).
58. Dahm, G., Dilba, D., Engelage H. (2017) as well as Doelfs G. (2016).
59. See Kamp, M., Dämon, K. & Kuhn, T. (2017).
60. Although 89 percent of managers are aware of the cyber risk, only 39 percent see themselves as actually exposed to this danger, 40 percent have actually been exposed to it (KPMG (2015)(1), p. 7).
61. Bitkom (2015).
62. Advison (2017).
63. Betterley, R. S. et al. (2017), p. 10.
64. KPMG (2017), p. 28.
65. Fromme, H. & Gammelin, C. (2017).
66. Choudry, U. (2014), p. 29.
67. Allianz and AXA, according to KPMG (2017), p. 29.
68. KPMG (2017).
69. The estimate is for Germany, Austria and Switzerland, Ibid., p. 34.
70. See GDV (2017)(1) and GDV (2017)(2).
71. For an extensive discussion of the debate about the insurability of nuclear power plants in Germany, see Wehner, C. J. (2012).
72. See also Ewers, H. J. & Rennings, K. (1992).
73. STEP stands for Sociological, Technological, Economic and Political Change. See for example Fahey, L. & Narayanan, V. K. (1986).
74. Allianz (2017).
75. Erdland, A. (2017).
76. Bundesministerium des Innern (2009), p. 8.
77. Die Bundesbeauftragte für den Datenschutz und die Informationssicherheit (2017), p. 17.
78. BIGS (2017), p. 47ff.
79. Ibid.
80. Ibid. p. 52ff.
81. In Germany, the Deutsche Kernreaktor-Versicherungsgemeinschaft is a nuclear power plant insurance pool. It is a pool of insurers of German nuclear power plants and functions as a re-insurer, as traditional insurers exclude nuclear power.
82. BIGS (2017), p. 47ff.
83. Ibid. p. 52ff.
84. Ibid. p. 50
85. Ibid. p. 56
86. Ibid.
87. Ibid. p. 50
88. Ibid. p. 56
89. Ponemon Institute (2017)(1), p. 22, 28.
90. One example of this in Germany is the Allianz für Cybersicherheit (Alliance for Cyber Security).

REFERENCES

Advison (2017). Measuring Cyber Risk – Understanding the Right Data Sources. Webinar. Retrieved May 31, 2017 from http://www.advisenltd.com/2017/05/31/measuring-cyber-risk-understandingright-data-sources/.

Allianz (2017). Allianz Risk Barometer. Top Business Risks 2017. Retrieved July 20, 2017 from http://www.agcs.allianz.com/assets/PDFs/Reports/Allianz_Risk_Barometer_2017_EN.pdf

Allianz (2013). Allianz Risk Pulse. Focus Business Risks. Retrieved July 20, 2017 from http://www.agcs.allianz.com/assets/PDFs/Reports/AllianzRP-Risk%20Barometer%20Jan2013.pdf

Andelfinger, V. & Hänisch, T. (2017). Industrie 4.0. Wie cyber-physische Systeme die Arbeitswelt verändern. Wiesbaden: Springer Verlag.

Baban, C. P. & Stuchtey, T. H. (2014). Grundlagen für Risikoanalyse und Risikobewertung. In: Schreiber, J. (ed.): Sicherheit und Gefahrenabwehr bei Großveranstaltungen (pp 27-36). Edewecht: Stumpf+Kossendey.

Betterley, R. S. et al. (2017). The Betterley Report – Cyber/Privacy Insurance Market Survey – 2017 Rates Are Surprisingly Soft. Massachusetts: International Risk Management Institute. Retrieved July 17, 2017 from https://www.irmi.com/online/betterley-report-free/cyber-privacymedia-liability-summary.pdf

BIGS (2017). Cyberversicherungen als Beitrag zum IT-Risikomanagement - Eine Analyse der Märkte für Cyberversicherungen in Deutschland, der Schweiz, den USA und Großbritannien. Potsdam: Brandenburgisches Institut für Gesellschaft und Sicherheit. Retrieved October 16, 2017 from http://www.bigs-potsdam.org/images/Standpunkt/Standpunkt_8Cyberversicherungen _Bildschirmversion.pdf

Bitkom (2016). Kosten eines Cyber-Schadensfalles. Leitfaden. Retrieved July 5, 2017 from https://www.bitkom.org/noindex/Publikationen/2016/Leitfaden/Kosten-eines-Cyber-Schadensfalles/160426-LF-Cybersicherheit.pdf

Bitkom (2015). Digitale Angriffe auf jedes zweite Unternehmen. [Press release April 16, 2015] Retrieved July 18, 2017 from https://www.bitkom.org/Presse/Presseinformation/Digitale-Angriffe-auf-jedes-zweiteUnternehmen.html

Brinkmann, T. (1993). Leistungsspektrum und Funktion des Versicherungsmaklers. In: Beiträge über den Versicherungsmakler (pp. 65-77). Hamburg: Hamburger Gesellschaft zur Förderung des Versicherungswesens

Brück, T., de Groot, O. J. & Ferguson, N. (2014). Measuring Security. In: Caruso, R. and Locatelli, A. (eds.). Understanding Terrorism: A Socio-economic Perspective. Contributions to Conflict Management. Peace Economics and Development (Vol. 22, pp 69-95). Bingley: Emerald Group Publishing Ltd.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2014). Aufgaben und Ausstattung. Definition Kritische Infrastrukturen; Sektoren- und Brancheneinteilung. Retrieved July 31, 2017 from http:// www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Downloads/Kritis/neue_Sektoreneinteilung.pdf?__blob=publicationFile

Bundesamt für Sicherheit in der Informationstechnik (2016). Cyber-Angriffe auf Telekom: BSI fordert Umsetzung geeigneter Schutzmaßnahmen. [Press release November 28, 2016] Retrieved January 19, 2017 from https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/ Presse2016/Angriff_Router_28112016.html

Bundesamt für Sicherheit in der Informationstechnik (2014)(1). Die Lage der IT-Sicherheit in Deutschland 2014. BSI-LB15503. Retrieved July 17, 2017 from https://www.bsi.bund.de/SharedDocs/Downloads/ DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__ blob=publicationFile

Bundesamt für Sicherheit in der Informationstechnik (2014)(2). Empfehlung: IT in der Produktion. Industrial Control System Security. Top 10 Bedrohungen und Gegenmaßnahmen 2016. BSICS-005. Retrieved July 5, 2017 from https://www.allianz-fuer-cybersicherheit.de/ ACS/DE/_/downloads/BSI-CS_005.pdf?__blob=publicationFile

Bundesamt für Sicherheit in der Informationstechnik (n.d.). Themen. Retrieved July 5, 2017 from https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/cyber-sicherheit_node.html

Bundeskriminalamt (2015). Cybercrime Bundeslagebild 2015. Retrieved July 5, 2017 from https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2015.html

Bundesministerium des Innern (2009). Nationale Strategie zum Schutz Kritischer Infrastrukturen Retrieved July 5, 2017 from https://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2009/kritis.pdf?__blob=publicationFile.

Choudry, U. (2014). Der Cyberversicherungsmarkt in Deutschland. Eine Einführung. Wiesbaden: Springer Gabler.

Dahm, G., Dilba, D. & Engelage, H. (2017). Cyber Security – IT Risiken für den Mittelstand erkennen, vorbeugen, versichern. Berlin: Gesamtverband der Deutschen Versicherungswirtschaft e.V. GDV. Retrieved July 20, 2017 from https://cybersecurity.gdv.de/

Die Bundesbeauftragte für den Datenschutz und die Informationssicherheit (2017). Datenschutz-Grundverordnung. Info 6. 3rd Edition. Bonn: BfDI.

Doelfs, G. (2016). "Lukaskrankenhaus Neuss – 900.000 Euro Gesamtschaden durch Cyberattacke," in: Das Gesundheitswirtschaftsmagazin/kma-online, June 24, 2016. Retrieved July 17, 2017 from https://www.kma-online.de/aktuelles/klinik-news/detail/900000-euro-gesamtschaden-durchcyberattacke-a-31629g

Erdland, A. (2017). Cyber-Kriminalität: dunkle Seite von Digitalisierung und Vernetzung. Speech presented at the GDV Cyber Security Conference, March 28, 2017. Retrieved July 20, 2017 from http://www.gdv.de/wp-content/ uploads/2017/03/Erdland_GDV_CyberKonferenz_Redemanuskript_2017.pdf

Erichson, S. (2016). Der Markt für Cyber-Versicherungen. Unterschiede und Stolperfallen. Speech presented at 14th Cyber-Sicherheits-Tag der Allianz für Cyber-Sicherheit – Versicherbarkeit von Cyberrisiken, Bayreuth, September 1, 2016.

Ewers, H. J. & Rennings, K. (1992). Abschätzung der monetären Schäden durch einen sogenannten Super-Gau. Basel: Prognos AG.

Fahey, L. & Narayanan, V. K. (1986). Macroenvironmental analysis for strategic management. St. Paul Minnesota: West.

FERMA (2016). European Risk and Insurance Report 2016. Federation of European Risk Management Associations. Retrieved July 20, 2017 from http://www.ferma.eu/app/uploads/2016/09/FERMA-European-risk-andInsurance-Report-2016.pdf

Fromme, H. (2017). WannaCry dürfte Cyber-Nachfrage pushen. In: Newsletter Versicherungsmonitor, May 15, 2017. Retrieved July 17, 2017 from http://versicherungsmonitor.de/2017/05/wannacry-duerfte-cyber-nachfrage-pushen/

Fromme, H. & Gammelin, C. (2017). Cyberversicherung: Attacke könnte Durchbruch bringen. In: Süddeutsche Zeitung, May 14, 2017. Retrieved July 17, 2017 from http://www.sueddeutsche.de/wirtschaft/2.220/cyberversicherung-attacke-koennte-durchbruch-bringen-1.3504726

GDV (2017)(1). Allgemeine Versicherungsbedingungen für die Cyberrisiko-Versicherung (AVB Cyber). Musterbedingungen des GDV, Stand April 2017. Retrieved July 20, 2017 from http://www.gdv.de/wp-content/ uploads/2017/04/AVB_Cyber_April_2017.pdf

GDV (2017)(2). GDV stellt Musterbedingungen für Cyberversicherung vor. [Press release, April 19, 2017] Retrieved July 20, 2017 from http://www. gdv.de/2017/04/gdv-stellt-musterbedingungen-fuer-cyber-versicherung-vor/ [Datum des Abrufs: 20.07.2017].

GDV (n.d.)(1). Zahlen und Fakten - Versicherungsbeiträge. Retrieved June 13, 2017 from http://gdv.de/zahlen-fakten/branchendaten/ueberblick/#versicherungsbeitraege

GDV (n.d.)(2). Zahlen und Fakten – Branchendaten - Überblick Versicherungsbeiträge. Retrieved July 24, 2017 from http://www.gdv.de/zahlen-fakten/ schaden-und-unfallversicherung/ueberblick/#beitraege-inkl-kraftfahrt

GDV (n.d.)(3). Zahlen und Fakten – Branchendaten – Versicherer. Retrieved July 24, 2017 from http://www.gdv.de/zahlen-fakten/branchendaten/versicherer/

Heidemann, J. & Flagmeier, W. (2014). Versicherungshandbuch. Betriebliche Versicherungen. Münster: Wolters Kluwer Deutschland.

Insurance Information Institute (2015). World Insurance Marketplace. Retrieved July 13, 2017 from http://www.iii.org/publications/insurance-handbook/economic-and-financial-data/world-insurance-marketplace

Kamp, M., Dämon, K. & Kuhn, T. (2017). IT-Sicherheit – Cyberversicherungen sind im Kommen. Wirtschaftswoche, May 21, 2017. Retrieved July 17, 2017 from http://www.wiwo.de/technologie/digitale-welt/it-sicherheit-cyberversicherungen-sind-im-kommen/19830220-all.html

KPMG (2017). Insurance Thinking Ahead. Versicherungen im Zeitalter von Digitalisierung und Cyber. Retrieved July 12, 2017 from http://hub.kpmg.de/cyber-risiken-versicherer?utm_campaign=Digitalisierung%20%26%20Cyber&utm_source=AEM.

KPMG (2015)(1). E-Crime. Computerkriminalität in der deutschen Wirtschaft. Retrieved July 17, 2017 from https://home.kpmg.com/content/dam/ kpmg/pdf/2015/03/e-crime-studie-2015.pdf

KPMG (2015)(2). Newsletter Forensic. Studie zur Computerkriminalität in Deutschland 2015. Retrieved July 17, 2017 from https://assets.kpmg.com/ content/dam/kpmg/pdf/2015/04/kpmg-forensic-newsletterapril-2015.pdf

List, T. (2015). Schutz vor Cyberrisiken. Nachfrage nach Deckungen wächst rasant. Börsen-Zeitung, September 30, 2015. Retrieved July 20, 2017 from https://www.boersen-zeitung.de/index.php?li=1&artid= 2015187017&titel=Schutz-vor-Cyber-Risiken

McAfee (2015). The Hidden Data Economy. Retrieved July 13, 2017 from https://www. mcafee.com/de/resources/reports/rp-hidden-data-economy.pdf

Naidu, R. & Das, A. (2015). ACE buys upmarket Chubb in biggest ever Insurance Takeover [Newswire Article July 1, 2015]. Retrieved July 5, 2017 from http://www.reuters.com/article/us-chubb-corp-m-a-ace-idUSKCN0PB4G220150701

Netdiligence (2016). Cyber Claims Study. Retrieved July 13, 2017 from https://netdiligence.com/wp-content/uploads/2016/10/P02_NetDiligence-2016-Cyber-Claims-Study-ONLINE.pdf

Ponemon Institute (2017)(1). 2017 Cost of Data Breach Study. Global Report. Retrieved July 20, 2017 from https://www.ibm.com/security/data-breach

Ponemon Institute (2017)(2). 2017 Cost of Data Breach Study: Country-specific Report for Germany. Retrieved July 20, 2017 from https://www.ibm.com/security/data-breach

Ponemon Institute (2016). 2016 Cost of Data Breach Study: Germany. Retrieved July 20, 2017 from http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094DEEN

Prokein, O. (2008). IT-Risikomanagement. Identifikation, Quantifizierung und wirtschaftliche Steuerung. Wiesbaden: Gabler Edition Wissenschaft.

Stuchtey, T. H. & Skrzypietz, T. (2014). Das Gut Sicherheit und die Rolle der Sicherheitswirtschaft bei seiner Herstellung. In: Apolte, T. (ed.): Transfer von Institutionen. Schriften des Vereins für Socialpolitik. (Vol. 340. pp. 193-212). Berlin: Duncker & Humblot.

Wehner, C. J. (2012). Grenzen der Versicherbarkeit – Grenzen der Risikogesellschaft. Atomgefahr, Sicherheitsproduktion und Versicherungsexpertise in der Bundesrepublik und den USA. In: Archiv für Sozialgeschichte (Vol. 52, pp. 581-605).

ABOUT THE AUTHORS

Dr. Constance P. Baban is a Senior Research Fellow at BIGS, where she heads the project "RiskViz – Providing a Risk Situation Picture of Industrial IT Security in Germany." After completing her Master of Arts in Linguistics, Political Science and Media and Communications Science, she earned a doctorate from the Leibniz Universität Hannover with a thesis focusing on Germany's domestic security policy. She is a Non-Resident Fellow in the Foreign and Domestic Policy Program at the American Institute for Contemporary German Studies (AICGS) at Johns Hopkins University in Washington D.C. and has several years of professional experience in security research, digitalization, and the public sector.

Yvonne Gruchmann is a Research Fellow at BIGS. Her work in the "RiskViz – Providing a Risk Situation Picture of Industrial IT Security in Germany" project is concerned with the risk analysis of cyber-physical systems, among other topics. She holds a degree in Economics, which she studied in Göteborg as well as Potsdam, with a special focus on empirical economic research. She has also worked as a research assistant at the chair of Public Finance at the University of Potsdam, German Institute for Economic Research (DIW) and Potsdam Institute for Climate Impact Research (PIK).

Dr. Christopher Paun is a Senior Research Fellow at the Brandenburg Institute for Society and Security (BIGS) in Potsdam. His main research interest is cooperation for the provision of security, including international, inter-agency and public-private cooperation. He completed his doctoral research at the Bremen International Graduate School of Social Sciences (BIGSSS), after having studied International Relations, Political Science and Cultural Studies in Frankfurt (Oder), Potsdam, Berlin and Washington D.C.

Anna Constanze Peters is a Junior Research Fellow at BIGS where she is part of the research project "RiskViz – Providing a risk situation picture of industrial IT security in Germany". She earned her bachelor's degree in International Business in Cologne and the Philippines. After working for McKinsey & Company, she earned a degree in Business Administration from the University of Potsdam. She also earned a second master's degree in International Climate Policy and Sustainability from the University of Leeds.

Dr. Tim H. Stuchtey studied Economics at the University of Münster and completed his doctoral degree at the Technische Universität Berlin. He has been the Executive Director of BIGS since 2010, where his research focus includes the economics of security. Stuchtey previously held a number of positions including Program Director Business and Economics of the American Institute for Contemporary German Studies (AICGS) at Johns Hopkins University in Washington, D.C. and chief of staff of the office of the president of Humboldt-Universität zu Berlin.

BIGS
BRANDENBURGISCHES INSTITUT
für GESELLSCHAFT und SICHERHEIT

IMPRINT

Located in Potsdam, the Brandenburg Institute for Society and Security is an independent, non-partisan, non-profit organization with an inter- and multidisciplinary approach with a mission to close the gap between academia and practice in civil security. The views expressed in this publication are those of the author(s) alone. They do not necessarily reflect the views of the Brandenburg Institute for Society and Security (BIGS).

Authors: Dr. Constance P. Baban, Yvonne Gruchmann, Dr. Christopher Paun, Anna Constanze Peters, Dr. Tim H. Stuchtey

Title: Cyber Insurance as a Contribution to IT Risk Management. An Analysis of the Market for Cyber Insurance in Germany

Editor: Brandenburgisches Institut für Gesellschaft und Sicherheit gGmbH (Brandenburg Institute for Society and Security)
Dr. Tim H. Stuchtey
(responsible according to the German press law)

BIGS Policy Paper No. 7, December 2017
Frontcover: Rajesh Rajendran Nair © 123RF.com

This publication was made possible through the financial support of the Federal Ministry of Education and Research of Germany.
ISSN: 2194-2412

Copyright 2017 © Brandenburgisches Institut für Gesellschaft und Sicherheit gGmbH. All rights reserved. No part of this publication may be reproduced, stored or transmitted in any form or by any means without the prior permission in writing form from the copyright holder. Authorization to photocopy items for internal and personal use is granted by the copyright holder.

Brandenburg Institute for Society and Security
Executive Director: Dr. Tim H. Stuchtey

Dianastraße 46 . 14482 Potsdam
Tel.: +49-331-704406-0 . Fax: +49-331-704406-19
E-Mail: info@bigs-potsdam.org . www.bigs-potsdam.org

BIGS
BRANDENBURGISCHES INSTITUT für GESELLSCHAFT und SICHERHEIT