Cyber Risk Management – a framework for companies to react to a constantly changing risk including a supply comparison of the German insurance market

Master's Thesis

submitted to

Prof. Dr. Jörg Schiller
Chair for Insurance Economics and Social Security
Institute for Health Care & Public Management
University of Hohenheim
Stuttgart

Edited by:
Christoph Rudolf Bechtle
Stationenweg 7
72818 Trochtelfingen
Phone: 0176 / 47779685
eMail: christoph.bechtle@uni-hohenheim.de
Study field: Management
Subject-related semester: 4
Matriculation number: 618 353

04.09.2019

Table of contents

List of Figures

List of Tables

List of Abbreviations

BDSG	Federal Data Protection Act
BSIG	Act on the Federal Office for Information Security
DDoS	Distributed-Denial-of-Service
GDPR	General Data Protection Regulation
GDV	German Insurance Association
IDC	International Telecommunication Union
ISO	International Organization for Standardization
ROSI	Return on investment for a security investment
SME	Small and Medium Enterprises
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union

List of Symbols

A	Primary loss
B	Sekundary loss
d	Deductible
P	Insurance premium
p_i	Probability of occurrence of condition i
r	Maximum value of the expected costs
α	Regression coefficient of the vector variable
β_i	Regression coefficient of the variable i
λ_t	Vektor of year variables
ε	Error term
ρ_{ind}	Vector of industry binary variables
σ	Risk of cyber attacks

1. Introduction

Almost every company has to deal with digitalization to work more efficiently, to produce cheaper or to maintain a competitive edge. The business world is changing. Cloud computing, blockchain, autonomous driving, and artificial intelligence influence business processes and create new opportunities. What does this development mean for the risk management of companies? What new risks have been created by new opportunities? And most importantly, how can the executive directors or risk managers protect their company against these threats? Which elements need complete cyber insurance? And which preconditions need to be fulfilled?

The value of data is steadily increasing and companies are using this information in all business processes.[1] The flip side of the medal is a growing invisible danger whose consciousness needs to be increased. Cyber attacks are the most likely technological risks in 2019, simultaneously creating the biggest impact.[2] On the one hand, productivity losses can occur. On the other hand, sensitive information can fall into the wrong hands resulting in high financial liabilities and reputation damage.[3] Estimating this intangible danger causes great problems for entrepreneurs, many of whom underestimate the danger and perceive it as given. Using a structured approach, the specific risk is to be assessed in order to take appropriate measures, since it is not possible to fully circumvent the digital risks. The aim of this master's thesis is to highlight the importance of incorporating cyber risks into the risk management process and to highlight the possibilities of cyber insurance. Cyber Risk Management is a topic that can be analyzed from different perspectives. In the further work, the focus is set explicitly on the possibilities of companies to deal with the risk in order to counter this growing danger. On the basis of current studies, the influence of the General Data Protection Regulation (GDPR[4]) and the connection between the GDPR and cyber attacks are examined. The GDPR has brought the increasingly connected entrepreneurial world even closer together through legal requirements. This impact on risk management should be explained in particular. Afterward, various measures are discussed to reduce the overall risk

[1] See Sharma et al. (2014), p. 437.
[2] See World Economic Forum (2019a), p. 5.
[3] See Abawajy (2014), p. 237.
[4] GDPR in the version of 04.05.2016.

of cyber threats. At the end of the work, the current market situation is presented and strengths and weaknesses are analyzed. Finally, a framework should be created to help entrepreneurs to use the right tools in order to reduce the overall cyber risk.

2. Risk Management and transformation

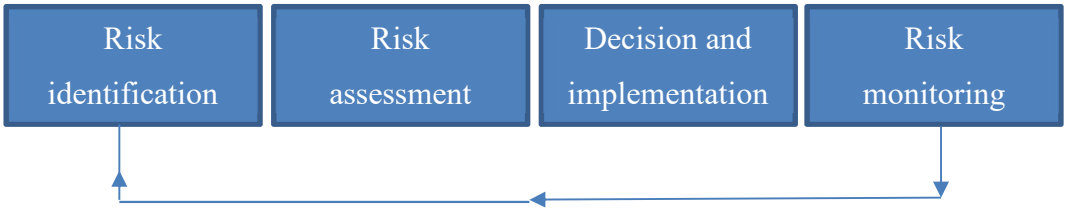
2.1 Classic Risk Management

Since the further work deals with the risk management of cyber attacks, it is important to begin with the main focus of classic risk management. In the next subchapters, the various risk types of companies will be discussed and the impact of the progressive digitization identified. There are many different definitions of risk and risk management in the academic literature. For example, the risk is the identification that there is a likelihood of a hazard in an economic decision.[5] Mc Neil et al. (2015) defined risk as "any event or action that may adversely affect an organization's ability to achieve its objectives and execute its strategies"[6]. In the globally valid standard ISO 31000:2018, published by the International Organization for Standardization, there are more general definitions. The scope of the standard is to settle rules for handling the risks in companies.[7] First of all, the risk is the "effect of uncertainty on objectives"[8]. According to this definition, the result of risky positions can be either positive or negative and reflect a more complete statement. Subject to the standard, risk management includes "coordinated activities to direct and control an organization with regard to risk"[9]. A further definition indicates that risk management is the process of consciously assessing future risks in order to take risks where future events may have adverse effects.[10] This more negative perspective deals with the fact that risk management creates the opportunity to reduce the risk by hedging the possible hazard with suitable instruments.[11] However, risk department employees can only hedge the risks they are aware of. Therefore, it is essential at the beginning of the risk management process to become aware of what can harm the company, how likely these situations are and what the consequences

[5] See Gabler Wirtschaftslexikon (2018).
[6] McNeil et al. (2015), p. 1.
[7] See International Organization for Standardization (2018).
[8] International Organization for Standardization (2018) clause 3.1.
[9] International Organization for Standardization (2018) clause 3.1.
[10] See Kloman (1990), p. 201.
[11] See Kaplan and Garrick (1981), p. 12.

are.[12] The risk has to be identified and potential scenarios estimated to manage future uncertainties.[13] Awareness is the foundation of risk management, but in the second step, explicit options for action must be discussed. In order to adequately respond to the specific risk, the probability and consequences of risk factors must be assessed.[14] Feasible options must be considered and the trade-off weighed in terms of benefits, costs and residual risks. Depending on the risk, various actions are possible to reduce or eliminate the risk. Strategies in risk management include risk transfer, risk-taking, risk elimination, risk reduction or further analysis of individual risks.[15] In addition, the influence on future options has to be considered in order to manage the company in a sustainable way.[16] After all, neither the company itself nor the environment is static and new types of risk can arise and the probabilities and consequences can change. To constantly recognize this, it is important to observe these changes and to change the risk assessment accordingly.[17]

Fig. 1: The risk management process[18]



Therefore, I can define a holitic risk management as a process that requires some basic elements as represented in Figure 1: First the risk must be identified, second the risk must be assessed, thirdly the risk management actions are discussed and implemented, and afterward, the different risk types have to be monitored to react to possible changes.[19]

Finally, the sub-chapter is completed, with the purpose of risk management. Eliminating or reducing risky positions is not the only academic and economic reason to manage risks. Beyond that, risk management can increase the value of the company. For example, risk management can reduce the volatility of corporate profits. Firstly, predictable earnings are a positive signal on the capital markets and secondly,

[12] See Kaplan and Garrick (1981), p. 13.
[13] See Hallikas et al. (2004), p. 52.
[14] See Hallikas et al. (2004), p. 53.
[15] See Hallikas et al. (2004), p. 54.
[16] See Haimes (1991), p. 169.
[17] See Hallikas et al. (2004), p. 54.
[18] Source: Own representation based on Hallikas et al. (2004), p. 52.
[19] See Hallikas et al. (2004), p. 52.

having a progressive tax rate, it reduces the amount of tax payments. Furthermore, lowering future tax payments increases today's firm value.[20]

A second opportunity to create value due to risk management is achieved via reduced bankruptcy costs. Risk management reduces the probability of default[21] or in other words, it reduces the probability of incurring bankruptcy costs.[22] A firm managing its risk is better prepared for potential changes and problems and can react faster or even prevent them. A further possible increase in value can be illustrated through the decreasing costs of capital.[23] On the one hand, risk management enables more debt financing and, on the other hand, it is more attractive to investors. The last reason for increased firm value through risk management are the reduced labor costs due to low fluctuation. Employees who participate in the company profit prefer a less volatile one and therefore, recruitment costs are reduced due to decreasing fluctuation.[24]

2.2 Financial Risks

Financial risks are the core of traditional risk management, as it is associated with the uncertainty of the financial outcome.[25] This type of risk results in a direct financial impact.

Examples of financial risks include market price risks, default risks, liquidity risks, and operational risks.[26] Firstly, these risks are briefly explained. Market risks are the risks of market price movements, which alter the financial portfolio of the company.[27] Examples of factors determining market price risks are interest rates, foreign exchange rates, equity prices, and commodity prices.[28] The risk of a counterparty not fully or legally fulfilling its obligations is default risk.[29] Depending on the company, these risks should be largely limited in risk management in order to not endanger operating results. Hence, the treasury department is considered as a cost unit in most companies. Financial companies exhibit specific characteristics, as

[20] See Christoffersen (2012), p. 4 and Smith and Stulz (1985), p. 392.
[21] See Christoffersen (2012), p. 4.
[22] See Smith and Stulz (1985), p. 392.
[23] See Christoffersen (2012), p. 4.
[24] See Christoffersen (2012), p. 4.
[25] See Bouchaud and Potters (2000), p. 91.
[26] See Albrecht (2003), p. 3.
[27] See Bank for International Settlements (2006), p. 157.
[28] See Christoffersen (2012), p. 6.
[29] See Christoffersen (2012), p. 6.

their operating business consists of entering into market risks.[30] However, the risk is also managed there and the company is hedged in its entirety. Furthermore, they have special regulatory conditions, e.g. Basel or Solvency.

In regard to management ratios or financial instruments, the risk is measured by the volatility.[31] Usual measures for the financial risks are the distribution of losses and the Value-at-Risk. The Value-at-Risk provides the entity with a probability estimate of which loss will not be exceeded in the next K trading days at a given level of significance.[32] Although financial risks affect every company, they and their associated risk management methods are not considered in detail, thus the focus is on operational risks and in particular cyber risks. In this regard, operational risks are also considered and treated as a separate type of risk.

2.3 Operational Risks

The Basel Committee on Banking Supervision defines operational risk as the "risk of loss resulting from inadequate or failed internal processes, people and systems or from external events"[33]. In the legal sense of Basel II, operational risk "includes legal risk, but excludes strategic and reputational risk"[34]. Basically, operational risks are risks that can arise in the course of business, regardless of the core activity.[35] To review the idea that cyber risks can be considered as a subset of operational risk according to the definition of operational risks, firstly the definition of cyber risks needs to be reviewed. Since the term cyber occurs explicitly or implicitly in every definition, this concept is considered first. Cyber is the short form of cyberspace and includes a virtual existing world, the hardware needed for it, as well as the internet itself.[36] In this regard, the term "cyber" is characterized in particular by the virtual conditions as well as electronic communication technology.[37] Cyber risks are intentional, targeted and IT-based attacks on data and IT systems.[38] This

[30] See Christoffersen (2012), p. 6.
[31] See Bouchaud and Potters (2000), pp. 91f.
[32] See Christoffersen (2012), pp. 12f.
[33] Bank for International Settlements (2006), p. 144.
[34] Bank for International Settlements (2006), p. 144.
[35] See Seibold (2006), p. 9.
[36] See Gabler Wirtschaftslexikon (2019).
[37] See Eling and Schnell (2016), p. 476.
[38] See Gabler Wirtschaftslexikon (2019).

definition doest not capture the entirety of cyber risks. In the further sense of the work, the definition is extended accordingly as can be seen below.

Risk of loss resulting from attacks on the informational technology or operator errors, affecting the IT system, database, manufacturing or services of a company.

Comparing the definition of operational risks with the characteristics of cyber risks, there are several overlaps and cyber risk should be consideres as a part of the operational risk of a company. This partition makes sense due to the impact of cyber risks to other operational risks e.g. supplier risk, compliance risk, and reputational risks.

Cyber risks are also considered part of the operational risk in the scientific literature.[39]

Especially, cyber incidents e.g. due to a data breach or system failure lead to high financial or reputational losses.[40] Even new technologies do not provide a risk-free environment but create new risks from solved problems.[41] Therefore, a rapidly changing digital business environment also requires risk management that adapts to the ever-changing input factors. Companies deal with cyber risks since the launch of the internet and the connected problems, as well as the point of view, changed steadily. Even in 1992, the findings proposed that in a digital landscape the corporate governance have to deal with security breaches, have to be aware of laws and potential fees and manage the digital risk in the overall context of the firm's risk management.[42] Cyber risks differ mainly by two characteristics. On the one hand, the IT system of a company has to be seen as a unit. The network consists of a large number of components that are linked together. Individual weak points weaken the network through the interrelation. Furthermore, information technologies are needed throughout the entire value chain, so a failure leads immediately to large losses.[43]

From this chapter results, if the operational risk is mentioned afterward, this includes, contrary to Basel II definition, strategic and reputational risk. Consequently,

[39] See Mukhopadhyay et al. (2013), p. 12.
[40] See Biener et al. (2015b), p. 131.
[41] See Kloman (1990), p. 204.
[42] See Loch et al. (1992), p. 185.
[43] See Böhme and Schwartz (2010), p. 5.

cyber risk can be considered as a subset of operational risk. The acceptance of financial risks is also an opportunity due to the neutral character risk and can create an additional return. In contrast, operational risks should be minimized and eliminated as there is little or no return for companies.[44] The only possibility to benefit from accepting operational risk is to save the costs that would be needed to minimize or eliminate risk.

2.4 Taxonomy of Cyber Risks

In reality, there exist multifaceted forms of cyber attacks. Therefore, it is necessary to divide it up into theoretical groups. It is important to be aware of this different origin because only then, you can react adequately or act proactively at best.[45] According to the academic literature, Jouiani et al.[46] split the security threat of cyber attacks up, into the source of the attack, the agents enabling the threat, the motivation behind the attack, the intention of the attacking people and the impact of the threat. In this model, the source of a threat can be within the company or extern. They distinguish the agents in human-made threats, environmental threats, and technological threats. By definition, environmental threats and technological threats are non-malicious and accidental, whereas human-made threats can be either malicious or non-malicious and either accidental or intentional. The impact of the threat can correspond to every origin of the danger and can be subdivided into seven types: Information can be destroyed, infected, stolen, disclosed, encrypted, accessed or used illegally. Applied on cyber security, examples for human threats are employees or hackers, for an environmental threat are natural disasters impairing the information systems and technological threats are e.g. the damage of the hard- and/or software. Cebula and Young (2010) define the cyber risk as operational risks to information and technology assets that hinder or inhibits the availability of information or information systems. [47] Moreover, the confidentiality or integrity of the stored information is endangered due to an incident.[48] As mentioned before, classification is important, to individually manage this multitude of possible risks. Since Cebula and Young (2010) explicitly classify individual points of interest in a

[44] See Christoffersen (2012), p. 7.
[45] See Jouiani et al. (2014), p. 491.
[46] See Jouiani et al. (2014), p. 492.
[47] See Cebula and Young (2010), p. 1.
[48] See Cebula and Young (2010), p. 1.

different way, which will be considered in more detail in the further work, this classification will be briefly explained. The complete classification is illustrated in Appendix 1.[49] The identified groups are: actions of people, systems and technology failures, failed internal processes, and external events. Each group has subordinated categories which are declared by explicit cases of damage. In the group action of people, they distinguish between an unintended action without malicious intent, an intended action with malicious intent and a lack of action where people fail to act when they should. In category two, there are systems and technology failures. There are associated failures in physical equipment, software assets and integrated systems. Thirdly, failed internal processes can lead to cyber risks e.g. failure of processes, inadequate controls on the operation of the processes and failure of organizational supporting processes, which deliver the appropriate resources. In the last category, external events are summarized: Natural disasters, legal issues, business issues and the dependence on external parties can be the reasons for cyber threats. In the later work, this classification will be reassessed and compared with current dangers.

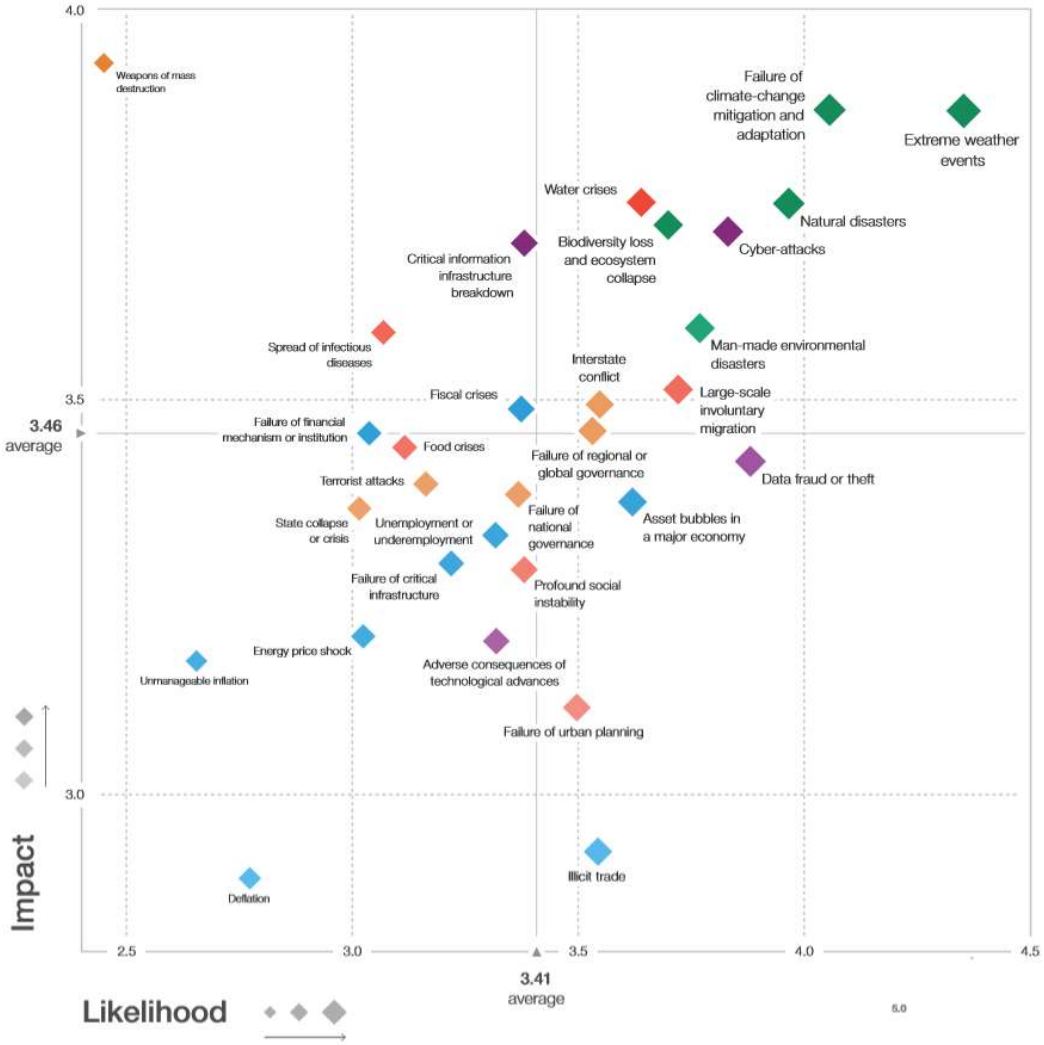
2.5 Quantifying Cyber Risks

2.5.1 Probability and impact in comparison to other risks

As mentioned in the introduction, the resulting threat from technologies and the networked world continues to evolve. Cyber risks are therefore no longer seen as a marginal problem but as a serious risk with profound impacts. This is confirmed by the study of the World Economic Forum. The Global Risks Report 2019 summarizes annually the current global risks and represents the results in a diagram, which shows the relative relationship between risks in regard to impact and probability. This diagram is illustrated in Figure 2. The positioning of the risks based on the assessment of approximately 1,000 experts and reflects specialization.[50] The allocated color represents the grouped category. Thus, the blue quadrangle illustates an economic risk, the green quadrangle illustates an environmental risk, the yellow quadrangle illustrates a geopolitical risk, the red quadrangle illustrates a societal risk and purple quadrangle represents a technological risk.

[49] See Appendix 1: Taxonomy of Cyber Risks.
[50] See World Economic Forum (2019b).

Fig. 2: Risk Map 2019 in regard to probability and impact[51]



The diagram is an extract of the complete scale, where 0 is the smallest size and 5 is the maximum. The likelihood of an occurrence is plotted on the X-axis and the impact of an occurrence is plotted on the Y-axis. The crucial finding of the study is that cyber attacks are estimated to be the most likely technological risk and, at the same time, the risk with the highest impact. Proceeding findings include that the impact of data fraud or theft is identified as relevant in the context of probability. The relationship between cyber attacks and customer data will be discussed in a later chapter. Concluding this overview, the impact of cyber attacks on the global economy is compared to some other risks to illustrate the extent. The impact of cyber attacks is larger than consequences from food crisis, fiscal crisis, and inter-state conflicts.

[51] Source: World Economic Forum (2019a), p. 5.

Up to this point, cyber risk can be characterized as a complex risk with multiple causes, high probability, and high impact. To understand the risk more deeply, some developments and characteristics are considered in more detail. In particular, cyber risks differ from traditional business risks through the fact that attackers are not regionally settled and can interact from everywhere, the extent of an attack is not bounded to the attacked device but can affect the entire company, and the attack occurs undetected in the first instance.[52] Another major difference is the mutation of cyber risk over time. Both the cause of a cyber attack and the associated damage probability and scope of damage change over time. For example, autonomous driving is a new target of a cyber attack. For this reason, automobile insurance sometimes already contains an insuring clause that safeguards damage through intervention or manipulation of the vehicle software by an unauthorized third party.[53] This exemplary development will be repeated and developed over the next few years with continous new technologies e.g. artifactual intelligence.

2.5.2 Academic Models and practical implementation

After classifying cyber risks into operational risk, discussing the sub-types of possible types of cyber incidents, and record the importance of cyber risks, this section presents the practical and scientific methods for quantifying cyber risks. In the first step, the Basel Committee suggeste a simple benchmark to determine a required capital buffer in order to meet the regulatory requirements against operational risks.[54] This benchmark determines the amount of required regulatory capital in relation to the size of the institution. The size can be measured at economically management ratios e.g. the gross revenue or the total assets.[55] The relative capital charge is determined by a fixed percentage set by the Basel Committee.[56] The described Basic Indicator approach follows the assumption that operational risk increases relative to the size of the institution but does not distinguish between the various types of operational risk. Two other approaches, proposed by the Basel Committee on Banking Supervision, are the Standardized Approach and the Advanced Measurement Approach. The Standardized Approach divides the institution partition into

[52] See Gordon et al. (2003), p. 82.
[53] See for example Allianz (2018) p. 8, Clause 1.3 (4).
[54] See Basel Committee on Banking Supervision (1999), p. 50.
[55] See Basel Committee on Banking Supervision (1999), p. 50.
[56] See Bank for International Settlements (2001), p. 8.

eight lines of business and for every single line of business, the representative financial ratio is multiplied with a specific coefficient.[57] The advantage compared to the Basic Indicator Approach is that different ratios, as well as different coefficients, can be used, depending on the business line. The third suggested approach is the Advanced Measurement Approach. Applying this approach, an institution needs an internal risk measurement system, which includes qualitative and quantitative standards. The required capital is estimated with the internal risk and the Standardized Approach is used as a comparative value.[58] The Advanced Measurement Approach is based on the assumption that the internal risk systems can best assess individual risk.

In addition, scientific publications have produced two approaches that model operational risk. On the one hand, "Top Down" models estimate the operational risk as a whole. On the other hand, in "Bottom-Up" models the operational risk for individual business units or individual processes is determined.[59] Looking at cyber risks in this regard, bottom-up models can better quantify corporate risk, since the individual processes are individually examined and then aggregated. Although these models are more elaborate and expensive, the advantage is that Bottom-up methods reveal the main points of attack of every business process, thus enabling better corporate management and planning.[60] In scientific literature, statistical methods are used to estimate the loss distribution. Statistical models estimate the probability distribution of losses, through analyzing available and relevant data. The difference consists of the possible input factors. Whereas Actuarial Models are based on a quantitative approach, Causal Models are based on causal relationships between input factors and losses and Bayesian Models combine qualitative and quantitative data.[61] The three identified model variants are summarized in Table 1.

[57] See Bank for International Settlements (2001), p. 6.
[58] See Bank for International Settlements (2001), p. 5.
[59] See Smithson and Song (2000), p. 58.
[60] See Cornalba and Giudici (2004), p. 167.
[61] See Cornalba and Giudici (2004), p. 169.

Table 1: Bottom-Up approaches to quantify operational risks[62]

Process approach	Factor approach	Actuarial Approach
• Causal networks • Fuzzy logic • Bayesian belief networks • Statistical quality control and reliability • Connectivity • System dynamics	• Predictive Models	• Empirical Loss distributions • Explicit distributions parameterized using historical data • Extreme value theory

As previously justified, Table 1 only includes Bottom-Up Models to quantify operational risk because this approach is more appropriate to deal with cyber risks of companies.

2.5.3 Allocation of Costs

As cyber attacks illustrate a complex occurrence with several consequences, the associated losses will also be split up. To understand the various types of losses due to a cyber attack, the different origins have to be distinguished. Therefore, Bandyopadhyay et al. (2009) differentiate between a symptomatic and systemic breach of security. If attackers utilize weaknesses of a specific company, the attack is a symptomatic breach. If the attack could not have been prevented, then it is a systematic breach instead.[63] Another important differentiator is the publicity of an incident. An attack whose effects are visible to the public or made visibly must be differentiated from a private attack.[64]

[62] See Smithson and Song (2000), p. 58.
[63] See Bandyopadhya et al. (2009), p. 69.
[64] See Bandyopadhya et al. (2009), p. 70.

In this regard, there are two types of possible costs. First of all, the intangible nature of cyber losses cause problems in assessing the losses.[65] Primary losses are traceable costs resulting from a cyber attack. Therefore, primary losses always arise in a successful attack, regardeless of the previously written properties.[66]
Furthermore, possible additional losses can result from a security breach. The breach initiates secondary losses that develop in succession and are not directly measurable.[67]
Romanosky (2016) developed subsequent model estimating the statistical relevant factors, which determine the costs of a cyber incident.

Equation 1: Model estimating the relevant cost factors[68]

$$\log(cost_{it}) = \beta_0 + \beta_1 * \log(revenue_{it}) + \beta_2 * \log(records_{it}) + \beta_3 * repeat_{it} + \beta_4 * \text{malicious}_{it} + \beta_5 * lawsuit_{it} + \propto * FirmType_{it} + \lambda_t + \rho_{ind} + \varepsilon_{it}$$

In this model, $cost_{it}$ is the total cost of a cyber incident of firm i in the year t, $revenue_{it}$ is the revenue of the firm, $records_{it}$, is the affected data of the firm, $repeat_{it}$ is a binary variable which is 1 if the firm was affected by more than one incident and 0 otherwise, $malicious_{it}$ is a binary variable which is 1 if the attack had a malicious intent and 0 otherwise, $lawsuit_{it}$ is a binary variable which is 1 if the attack initiated a lawsuit and 0 otherwise, $FirmType_{it}$ is a vector of binary variables which defines the type of the company and distinguish between a government agency, nonprofit, privately held company, or publicly traded company. Finally, the model is completed with two more factor variables which define the year and the industry, and an error term ε.
Table 2 summarizes the regression results. Doing this, only the statistically significant and economic reasonable results are listed.

[65] See Eling and Schnell (2016), p. 476.
[66] See Bandyopadhya et al. (2009), p. 70.
[67] See Bandyopadhya et al. (2009), p. 70.
[68] See Romanosky (2016), p. 130.

Table 2: Selected regression results for Equation 1[69]

Log(costs)	
Log(revenues)	0.133**
Log(records)	0.294***
Observations	265
R^2	0.466

*** p < 0,01, ** p < 0,05, * p < 0,1.

Before presenting the key findings, some crucial information for interpreting the results need to be provided. Firstly, the dataset used does not include cost information on lost revenue, decreased market valuations, lost time, or reputation damage.[70] However, as these costs are central to the aggregate assessment of the cost of cyber attacks, it is more appropriate to identify the drivers of primary costs in this model. This kind of primary costs should be seen as a more general synonym for the previously defined primary losses. The regression results exhibit that there is a statistically significant relationship between the primary costs of a cyber incident and firm revenues. The relationship is significant on the 5 % level and the parameter value reveals that a 10 % increase of firm revenues leads to increasing primary costs of 1.33 %. Furthermore, the affected data influences the primary costs. The relationship is significant on the 1 % level and the parameter value is even larger, showing that a 10 % increase of firm revenues leads to increasing primary costs of 2.94 %. The determination coefficient R^2 shows that the model explains 46.6 % of the variance. In this regard, the model serves as a rule and sets the firm size and the affected company data as representative for the primary costs of a cyber attack. At this point it is important to highlight the difference, this model identifies the factors relevant to the level of costs, and does not provide a causal link for the cause.[71] Hence, it is not possible to reason that a larger firm is more likely affected by a cyber incident.

[69] Source: Own representation based on Romanosky (2016), p. 130.
[70] See Romanosky (2016), p. 129.
[71] See Romanosky (2016), p. 130.

The corresponding actuarial classifications are first-party losses and third-party losses.[72] This distribution of costs does not equate to the division of the primary and secondary costs, because the affected party is more relevant than the time. First-party losses are arisen costs, which affects the aggrieved company e.g. business interruption, forensic investigation costs, legal notification costs, marketing costs, and public relations costs.[73] The other type of losses arise in particular through private litigation or legal fines and replace the damage of another party.[74] Table 3 summarizes concrete costs that can arise from cyber risks.

Table 3: Possible costs due to cyber attacks[75]

First-party losses (property)	Third-party losses (liability)
• Costs due to business failure • Costs of IT-forensic • Costs of IT recovery • Cost of data recovery • Costs of crisis management • Reputational damage • Notifications cost • Monetary fine and contract penalty • Blackmail and manumission payment	• Claims arising from violations of privacy policy • Network security liability • Costs of IT recovery • Reputational damage • Notifications cost • Monetary fine and contract penalty • Blackmail and manumission payment

As already mentioned, most of the primary losses are directly measurable but reputational damage exhibits special characteristica. For example, an IT company can easily estimate the damage of a cyber attack, the notification costs arise after a certain process and the optional blackmail payments are determined by the blackmailer. Reputational damage, however, is more difficult to determine and to quantify. Basically, three factors determine the reputation risk. When a company is better perceived than it actually is, the reputational risk is larger. Secondly, if stakeholder greatly changes the expectations of the company the reputational risk increases and

[72] See Romanosky (2016), p. 129.
[73] See Romanosky (2016), p. 129.
[74] See Romanosky (2016), p. 129.
[75] Source: Own representation based on Biener et al. (2015a), p. 10 and Hiscox (2019b), pp. 4-10.

finally, the quality of internal coordination is decisive.[76] Therefore, reputational risk can be reduced, if a company reduces the resulting expectations or improves the ability to meet expectations.[77] To properly manage reputational risk, you need to be able to accurately assess the company's reputation, evaluate the true nature of the business, minimize the perceived difference in perceived and factual reputations, constantly monitor changing expectations, and hold a senior executive accountable.[78]

Reputational damage can lead to significant losses for the company. Examples include loss of current or prospective customers, loss of current or future business partners, loss of staff and associated personnel recruitment costs, increased financing costs and increased costs due to penalties and other legal regulations.[79]

As reputational losses reduce future cash flow or increase the required market return, one approach to evaluate the impact of reputational damage is to compare the share value of the company before and after a reputation diminished incident. Palmrose et al. (2004) found a statistically significant negative impact on the announcement.[80] In a two-day period, the cumulative abnormal mean return reduces by 9.2 %.[81] Even more important in the context of cyber risks is the impact of fraud disclosures in the company. Separating these incidents, the cumulative abnormal return has decreased by 20 %.[82] Therefore, when companies negligently deal with customer data and do not arrange sufficient security measures, the reputational damage caused by a cyber attack can be very large because stakeholder can question management integrity.

[76] See Eccles et al. (2007), pp. 2f.
[77] See Eccles et al. (2007), p. 4.
[78] See Eccles et al. (2007), p. 6.
[79] See Perry and de Fontnouvelle (2005), p. 5.
[80] See Palmrose et al. (2004), p. 60.
[81] See Palmrose et al. (2004), p. 69.
[82] See Palmrose et al. (2004), p. 71.

3. Different types of cyber attacks

3.1 Definition and description

Even from the previous categorization of cyber risks, it becomes clear that cyber risks can occur in different forms and happen for different reasons. Looking first at cyber attacks, it is a deliberate action, so a person wants to harm a company. So far, although the effects of cyber attacks have been presented, they have not been categorized correctly. According to German legislation, security in information technology means adhering to certain security standards relating to the availability, integrity or confidentiality of information.[83] Bedner and Ackermann (2010) expand the protection goals of IT security.[84] By definition, a cyber attack occurs when the information security protection goals are violated. Therefore, availability, integrity and/or confidentiality must be threatened or violated. There are several opportunities how a cyber attack can violate IT security. The most common variants are shown on the basis of a study by the Federal Office for Information Security.
Due to the ever-increasing danger, the Alliance for cyber security was founded by the Federal Office for Information Security in 2012. Up-to-date information, the exchange of knowledge and experience as well as the constant development of security competencies are intended to strengthen Germany's resilience to cyber attacks.[85] Since 2014, the Federal Office has been investigating in a Cyber Security Survey the risk assessment and actual attacks of German institutions through cyber attacks every year, as well as the status of implementation of corresponding protective measures.[86] Among other results, which will be discussed later, the results include the type of reported attacks in 2018.[87]

In 2018, 53% of reported cyber attacks were malware infections infiltrating corporate IT systems, 18% were DDoS attacks and only 12% were targeted hacking.[88] In order to better understand and deal with the main types, these forms are first defined and explained.

---

[83] See § 2 (2) BSIG.
[84] See Bedner and Ackermann (2010).
[85] See Federal Office for Information Security (2019a).
[86] See Federal Office for Information Security (2019b).
[87] See Federal Office for Information Security (2019b).
[88] See Federal Office for Information Security (2019b), p. 12.

- Malware: The generic term “malware” includes malicious software that gets into the IT system of the company. These classic forms of cyber attacks are all well-known, as they include, for example, viruses, worms, or Trojan horses.[89] Since the necessary knowledge is needed only in the creation and less in the use, malicious software is also resold, e.g. in the darknet.[90] Depending on the form, access to computer systems and network resources is possible after the infection has taken place. From this, the computer operation can be disturbed and personal information can be accessed and collected.[91] In particular, companies can protect themselves by using virus scanners. However, they only recognize known descriptions or signatures from a database. Therefore, a constant update is essential as new forms are created every day.[92] The ways vary how a company gets infected with the malware. Mainly, there are e-mail attachments that are opened. Of the aforementioned 53% malware incidents, 90% entered the company in this manner.[93]

- DDoS: Due to a Distributed Denial of Service (DDoS) attack, a requested service is no longer or only very limited available. The trigger is in most cases an overload of the IT infrastructure.[94] Therefore, a stream of packets is transmitted from different sources, which overcharge the processing capacity. A technological mechanism to protect against DDoS attacks are globally coordinated filters, which restrict access by router settings. However, the same problem exists with virus scanners, because preventive settings use signatures of known attacks. So, new attacks with new signatures cannot be prevented and preventive setting can never completely eliminate the threat.[95]

[89] See Bayer et al. (2006), p. 67.
[90] See Bayer et al. (2006), p. 67.
[91] See Gandotra et al. (2014), p. 56.
[92] See Bayer et al. (2006), p. 67 and Gandotra et al. (2014), p. 62.
[93] See Federal Office for Information Security (2019b), p. 12.
[94] See Douligeris and Mitrokotsa (2004), p. 643.
[95] See Douligeris and Mitrokotsa (2004), p. 655.

- Hacking: Hacking is the concept of unauthorized access to the IT system.[96] Therefore, targeted hacking is the intentional access to an IT system of a company by overpowering the IT security.

- Fraud: Examples for other cyber attack are Fake President cases. The approach of the attackers is based on an alleged instruction from the management to the employees. Employees receive an e-mail from the manager's address (possibly slightly modified) with the instruction of a bank transaction.[97]

Consequently, the type of an attack is irrelevant in terms of the data. Trough both, malicious software and taditional hacking, an attacker can access the company database. This unrestricted access enables to act with this information. It is then in the scope of action of the attacker what he does with the data e.g. delete, infect, steal, disclose, encrypt, or use illegally. Even DDoS Attacks are related to data because they can prevent data from being used. This shows impressively the interconnection between data fraud or theft and cyber attacks. Hence, the two most likely technical dangers, as identified in chapter 2.5.1, have to be considered simultaneously.

3.2 Examples of damage from practice

This chapter will briefly explain the introduced methods of attack based on a practical example. This should allow a better understanding and emphasize the relevance that even very powerful companies can be affected.
In 2010, the group of hackers “Anonymous” attacked big companies like MasterCard, Visa, and PayPal with a DDoS attack. As a result, their websites were down for days and the transaction network was significantly disturbed.[98] Classifying this incident and using the introduced criteria in chapter 2.4, it was an action by people with intended action and with a malicious purpose. Looking at the impact on the company data, it affected in particular the customers, who could no longer access the website.

[96] See Furnell and Warren (1999), p. 29.
[97] See KPMG (2017), p. 27.
[98] See KPMG (2017), p. 26.

Also in 2010, Google's internal system was infiltrated with Trojan malware. The attack was made possible by an employee who clicked on a link in an e-mail. Afterward, attackers infiltrated this computer and the whole Google system. [99] This incident shows that sometimes a malicious attack consists of a combination of intentional action and the wrong decision of an employee.

In 2014, malicious programs were used to steal 145 million eBay customer records, including e.g. names, encrypted passwords, e-mail addresses, birthdays, addresses, phone numbers.[100] Assigning the attack to the classes of cyber attacks, it was again a malicious intended action of people and private customer data was stolen.

In 2015, even the US Federal Department of Human Resources was affected by a malware attack, which obtained personal data from 21.5 million government employees and applicants.[101]

In 2016, the German automotive supplier Leoni AG was affected by a Fake President incident. Employees did not realize that the transfer order was not instructed by the management. Furthermore, employees did not act according to the internal work instructions which cost the company 40 million.[102] Consequently, the direct damage was further extended by consequential losses, for example, the share price fell as a reaction by more than 10%.

In 2017, the malicious software WannaCry has identified hundreds of thousands of computers, encrypted data and thus extorted cash payments. Other examples of this kind of ramsomware are Locky, NotPetya or Emotet.[103] In the logic of classification, it was a malicious intended action of people and private customer data was encrypted.

Although intentional actions by humans have preceded all of the examples, even unintentional actions by humans may have contributed, for example, by opening an attachment or carrying out the demands.

The above examples are only to summarize that the types of attacks can take different forms and companies of all kinds can be affected.

[99] See The Register (2010).
[100] See KPMG (2017), p. 26.
[101] See KPMG (2017), p. 26.
[102] See DerTreasurer (2017), p. 10.
[103] See KPMG (2019), p. 8, 61.

4. Data processing and General Data Protection Regulation

4.1 Value of the Data

The impact of data and the value of given data is crucial for companies in their daily business and to operate successfully. There are several academic models that show how data becomes knowledge. The main aspect is to reduce the variety of available data to a representative data set. Detecting existing patterns out of the reduced data creates a better understanding of the subgroup.[104] The various steps to convert data into knowledge, changed through the development of big data from the traditional information value chain to a more complex process.[105] Accordingly, information is first extracted from data to generate knowledge. With this understanding, the quality of decisions can be enhanced, ultimately increasing the likelihood of the right action.[106] If a company makes high-quality decisions in the longer term, this will increase the value of the company.[107]

Big Data is characterized by the increasing data volume, faster data creation and a variety of types.[108] Therefore, the available data is increasing every day, from around 33 zettabytes in 2018 to an estimated size of around 175 zettabytes in 2025.[109] That corresponds to an annual growth rate of all data of 30 percent between 2018 and 2025. According to a further study of the IT market research company International Data Corporation, will already be created 79.4 zettabytes of data by the connected Internet of Things devices in 2025.[110] Other findings of the study are that the biggest growth is occurring in the industry and automotive sector. Over the forecasting period, it estimates a compound annual growth rate of 60 % due to new intelligent devices and sensors that capture and store more and more extensive data.[111]

This means that the opportunities and knowledge a company can achieve is increasing enormously. The increasing data volume is equivalent to a required IT capability to process data. Furthermore, 30 % of the data will be generated by real-time

[104] See Fayyad et al. (1996), p. 29.
[105] See Abbasi et al. (2016), p. 5.
[106] See Abbasi et al. (2016), p. 6 and Sharma et al. (2014), p. 437.
[107] See Sharma et al. (2014), p. 437.
[108] See McAfee and Brynjolfsson (2012), p. 63.
[109] See International Data Corporation (2018), p. 6.
[110] See International Data Corporation (2019), p. 1.
[111] See International Data Corporation (2019), p. 3.

data in 2025.[112] More and more digital processes and systems are being used to help companies generate value from their data, by responding immediately to changes in the values recorded. Choi et al. (2017) support the hypothesis via regression results that increasing IT capability leads to rising profitability through increased competitive actions.[113]

4.2 Principles and introduction of the GDPR

In order to discuss the GDPR, the legal system of the European Union must first be explained. Legislative changes at European level are implemented in accordance with the Treaty on the Functioning of the European Union (TFEU[114]). According to Article 288 TFEU, the legislature has different forms of action. Relevant to the case under investigation is the distinction between regulations and directives. Regulations have a general effect and are direct, complete and legally binding for each member state. Directives are different in national implementation. There is a specific objective which has to be achieved. According to the Treaty on the Functioning of the European Union, the objective is binding but the specific choice of form and means may vary in every member state.[115] Directives define a goal and a timeframe in which the content must be transposed into national law. Therefore, the member states are obliged to take suitable and effective measures in the implementation.[116] This difference becomes more important if you make yourself aware of the fact that the predecessor of the GDPR was the European Data Protection Directive. So far, the directive has been implemented in all 28 countries by different legal cultures. In a European business world where borders are increasingly being abolished, uniformed data regulation is a necessary step to eliminate bureaucracy and legal uncertainty.[117] In April 2016, the GDPR was introduced as regulation and the legislation pursued the goal of uniformly regulating the data protection in Europe. A modified legal framework was established, resulting in a level playing field for the European market.[118] The implementation of the legal framework occurred on the 25th of March 2018. From this point, the regulation sets guidelines for the

[112] See International Data Corporation (2018), p. 13.
[113] See Choi et al. (2017), p. 8.
[114] TFEU in the version of 26.10.2012.
[115] See Article 288 TFEU.
[116] See Article 4 (3) TEU. TEU in the version of 26.10.2012.
[117] See Albrecht (2016), p. 288.
[118] See Albrecht (2016), p. 288.

collection and processing of personal data of individuals within the European Union. In principle, the processing of personal data is only lawful, if the data subject has given his consent, if processing is necessary under a contract with the person, if it is legally necessary, if vital interests are involved, if it is in the public interest or if it is required in the legitimate interest of a third party.[119] Other changes are for example the designation of a data protection officer. Conditional some circumstances, the designation of a data protection officer is necessary, who among other things, monitors compliance with the regulation.[120] This is necessary if the core activities of the controller or the processor consist of processing personal data referred to Articles 9 and 10 GDPR, the processing requires regular and systematic monitoring of the data or the processing is carried out by a public authority.[121] Since regulation can always be tightened by domestic regulations, the German Federal Republic has regulated in § 38 of the Federal Data Protection Act (BDSG[122]) the designation of a data protection officer for a non-public entity. The obligation also applies to small businesses, as far as they usually employ at least ten persons with the automated processing of personal data. If a company processes customer-based data with new technologies, and this may lead to a high risk of rights and freedoms, a data protection impact assessment according to Art. 35 GDPR is necessary. If this is the case, a German company has to provide a data protection officer, regardless of the number of employees.[123]

Pursuant to Article 33 (1) of the GDPR, in the case of a breach of personal data protection, the competent supervisory authority must be informed at the latest within 72 hours. This notification must include a description of the nature of the breach of protection, which also includes the category and number of persons, the privacy officer, the probable consequences and the actions taken.[124] If the injury causes a high risk for the personal rights and freedoms of natural persons, every single person concerned must be informed immediately. If this is too costly, this

[119] See Article 6 (1) GDPR.
[120] See Article 39 GDPR.
[121] See Article 37 GDPR.
[122] BDSG in the version of 30.06.2017.
[123] See § 38 (1) BDSG.
[124] See Article 33 (3) GDPR.

can be replaced by an adequate public announcement.[125] The GDPR has not only increased transparency but has also introduced stringent sanctions. Article 83 (1) GDPR calls for violations of this regulation to be "effective, proportionate and dissuasive"[126]. Fines will vary depending on the circumstances of the case.[127] For example, if the responsible legal person breaches the GDPR provisions of the rights of the data subject in accordance with Articles 8 – 22, the fine can amount up to € 20 million or, in the case of a business, up to 4 % of its total worldwide annual turnover for the previous financial year. The higher amount will be applied.[128]

4.3 Impact on Risk Management

As mentioned in chapter 4.1 the data created every day is steadily increasing. At the same time, this increases the threat of a cyber attack. The GDPR brings cyber security and compliance close together because every cyber attack is a potential attack on the data of the company. Traditionally both organizational units have been managed by various staff because the context was not seen together.[129] In fact, however, internal information and customer data are affected in most cyber attacks. Nevertheless, the implementation and compliance with the regulation are associated with some effort. Furthermore, it is part of risk management that laws and regulations are adhered to, and there are some effects on risk management after implementation.

For example, even small businesses have to deal with the designation of a data protection officer. Due to changes in liability for data breaches, caution must also be exercised when outsourcing business units.

Art. 32 (1) GDPR requires that the data processing ensures the confidentiality, integrity, availability, and resilience of the systems and the company needs the ability to quickly restore the availability to personal data in case of a physical or technical incident. An aspect in which data storage has to meet the legal requirements both from the legal and from the compliance point of view.

These regulatory conditions and the digital development leads to the trend that many companies outsource data storage to meet the high regulatory demands.

[125] See Article 34 (1), (3) GDPR.
[126] Article 83 (1) GDPR.
[127] See Article 82 (2) GDPR.
[128] See Article 83 (5) GDPR.
[129] See Zerlang (2017), p. 8.

Currently, 31 % of German companies use public cloud computing and the trend is rising.[130] However, privacy cannot be completely outsourced. If, for example, an external cloud provider or subcontractor is involved, data processors must ensure that processors have appropriate technical and organizational measures to ensure that the processing complies with the requirements of this Regulation and the protection of the rights of the data subject.[131] The basic prerequisite for this is a contract processing contract that has the minimum contents specified in Art. 28 (3) GDPR. Without these minimum details, the entire order processing is ineffective due to a lack of legal basis. According to Art. 82 GDPR, controller, and processors are jointly and severally liable for breach of the obligations listed in the GDPR for the non-material and material damages suffered by the person concerned. Joint and several liability mean that the injured party can claim the damage at his option either to the responsible person or to the processor, regardless of the liability for the damage. Exclusion of liability is only possible if involved contracting party can prove that they are not in any way responsible for the infringement of regulation.[132] All these changes, such as the provision of a data protection officer, timely notifications and joint liability for subcontractors mean that a clear response plan needs to be defined in the company, which clarifies responsibilities.

The General Data Protection Regulation cannot be considered separately from cyber attacks. The reasons for this are the goals and effects of cyber attacks. As the current examples in Chapter 3.2 show, customer data has been stolen, encrypted and/or published. Due to this overlap, companies must always comply with the GDPR in the context of cyber risks in order to meet the regulatory requirements.

After all, not only does the volume of data volumes change, but so does the legal basis and how data is stored and processed. The support of digital processes and devices leads to a great opportunity to generate even more value from the given data but also increases the associated risks, which must be considered accordingly in a holistic approach to risk management. In particular, growing technologies, such as the Internet of Things, will store more and more valuable data and consequentially, new risks will emerge.

[130] See Bitkom (2018a).
[131] See Article 28 GDPR.
[132] See Article 82 (3) GDPR.

5. Precautionary measures and status quo

5.1 Technological precautions

5.1.1 Technical consideration

In the previous part of the work, the focus was on the risks, costs and legal regulations of cyber risks. The aim of this chapter is to weigh the technical safety level required to counteract the danger. Basic technical security is essential for successful cyber-protection since without these precautions an insurer would not even take the risk.[133]

First of all, it has to be explained from which components complete cyber security actually exists. A detailed list of security components uses the International Telecommunication Union (IDC) to define cyber security.

> "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets."[134]

This detailed description best reflects the complexity that exists in reality. Therefore, it is adopted as the definition of cyber security. It becomes clear that various measures are necessary to address the various components that are described as assets. As a result, a company's assets may include the entire IT system including the telecommunications system, as well as personnel, infrastructure, applications, services, and the totality of processed information in the cyber environment.[135] The main objective is to ensure continuous accessibility and maintenance, with three sub-goals to be achieved: availability, integrity, and confidentiality.[136] It must be noted, that individual weak points weaken the entire network through the interrelation and therefore endanger the cyber security.

In Germany, there are legal regulations concerning IT security (BSIG[137]). Accordingly, security in information technology means adhering to certain security

[133] See for example Chapter 7.3.
[134] International Telecommunication Union (2008), p. 2.
[135] See International Telecommunication Union (2008), p. 2.
[136] See International Telecommunication Union (2008), pp. 2f.
[137] BSIG in the version of 14.08.2009.

standards relating to the availability, integrity or confidentiality of information, through security measures in information technology systems, components or processes, or when using information technology systems, components or processes.[138]

During the first development of the digital environment, it was possible to secure information security through physical and technical arrangements. Since then, new technologies and more interconnected concepts have changed the digital landscape, resulting in safety precautions beyond technical.[139]

Nevertheless, technological protection is the first step in every cyber security process. The first component of cyber security starts with physical control. This implies that the IT system is secured against environmental threats, e.g. that the server room is secured accordingly.[140] The next step is adequate hardware, which has to be upgraded with appropriated software. The safeguarding is based on basic security tools e.g. firewalls, network intrusion detection systems or anti-virus software.[141] The ways of working clarify the problem since mainly known attack signatures are identified and thus cyber attacks are prevented. This means that listed technologies only react to already known attacks.[142] The problem has already been briefly addressed when the possible types of cyber risks were introduced.

Therefore, system maintenance, regular updates, and administration is the main constituent of every security system. For example, the operating system should be updated, unneeded software should be removed, and the system should be controlled by an administrator.[143] A final component of technological assurance is regular data storage. Back-ups significantly prevent loss in the event of damage and ensure a quick resumption of business activity.[144]

Insurance companies presume this methodology and require antivirus software with a current database, every web-enabled hardware needs a firewall and a regular data storage, i.e. at least weekly data backups.[145]

---

[138] See § 2 (2) BSIG.
[139] See Wood (2004), p. 16.
[140] See Siegel et al. (2002), p. 44.
[141] See Siegel et al. (2002), p. 47.
[142] See Bandyopadhya et al. (2009), p. 68.
[143] See Siegel et al. (2002), p. 47.
[144] See Siegel et al. (2002), p. 48.
[145] See Appendix 2 or Chapter 6.3 for more information.

Comparing the technical consideration with the taxonomy of cyber risk there are some differences recognizable. In Chapter 2.4 human-made threats, environmental threats, and technological threats are identified as cyber risks. Comparing the source of dangers, a company can only reduce the extent of two danger due to technological precautions. Therefore, physical control restricts environmental threats and hardware with appropriated software limits technological threats. How human dangers are limited, however, is not easily answered by the technological precautions, for which the subspecies must be considered more closely.

At the end of this subchapter, the impact of cyber insurance on the technical equipment of companies is examined. There are three different scenarios possible: Taking out cyber insurance has a positive effect, a negative effect or no effect on the IT security level of companies.

The positive impact can be justified due to the academic view of cyber insurance. In an exemplary risk management process, the risk is firstly reduced with technological instruments. Furthermore, as insurance companies require specific precautions and updates, the insurance policy will lead to an improved IT system.

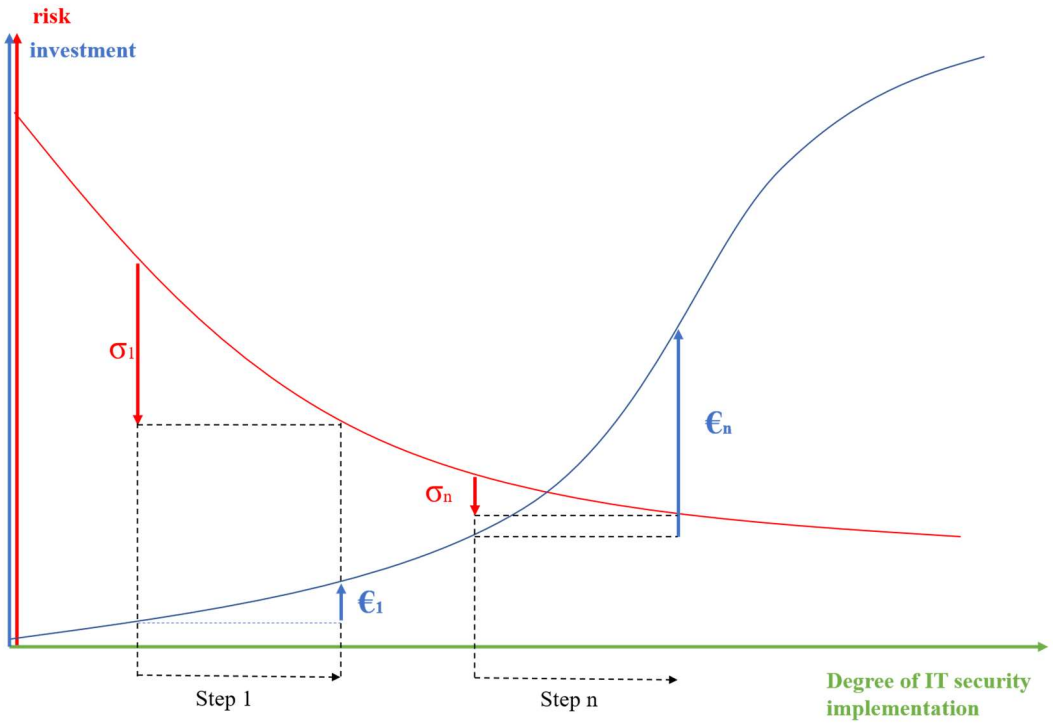
An argumentation for a negative impact includes especially the moral hazard problem. An insured company will be less concerned with IT security.[146] Empirical proof of the impact has not yet been recognized, however, by taking out insurance the awareness of IT security is strengthened and updates of the software are carried out, resulting in longer-term security.

5.1.2 Economically consideration

The last chapter identified technical requirements that reduce the risk of cyber attacks. This chapter considers the same content but from another perception, in regard to the economic effect. According to a representative survey, 74 % of German companies increase IT security spending.[147] This fact raises the question of how much risk reduction is achieved by investments in IT security, as business decisions should be particularly economically rational. Figure 3 shows the relationship between the investments in IT security and the connected risk reduction. The investments are indicated in € and the risk is illustrated with the Greek letter σ.

[146] See Gordon et al. (2003), p. 83.
[147] See Bitkom (2018b) p. 5.

Fig. 3: Economically contemplation of IT security investments[148]



The gradient of the risk graph shows that the extent of risk minimization does not increase linearly with the investment.[149]

If a company makes a security investment, the risk is disproportionately reduced. Figure 3 shows this relationship as $\sigma_1 > €_1$. However, if the company has reached a certain level of IT security, the impact of a further investment n differs. Risk reduction requires a significant investment because new, better and therefore more expensive hardware and/or software is needed. Consequential, the investment $€_n$ achieves a risk reduction σ_n, where $\sigma_n \ll €_n$.

Since the technological viewpoint cannot be fully assessed here, the context should only highlight the economic component. Even security investments have to make business sense.[150] If business investment no longer makes sense and managers are not forced to implement them, they should consider alternatives. One opportunity is illustrated in Equation 2. Therefore, the return on investment for a security investment (ROSI) is calculated.

[148] Source: Own representation based on Pohlmann (2006), p. 4.
[149] See Pohlmann (2006), p. 4.
[150] See Sonnenreich et al. (2006), p. 45.

Equation 2: Equation for calculating ROSI[151]

$$ROSI = \frac{(Risk\ Exposure * \%\ Risk\ Mitigated) - Solution\ Cost}{Solution\ Cost}$$

ROSI enables comparing a security investment based on an economic ratio. The cost of purchasing the hardware and/or software is weighted against the expected prevented loss. If the result is positive, an investment is economically reasonable. A limitation of the concept is that the factors regarding cyber risk are difficult to estimate and vary over time. Therefore, changing exposure costs can lead to misleading results.[152]

Another benchmark was already established by the Goerdon-Loeb Model in 2002.[153] With the assumption that cyber security investments have a diminishing marginal utility (as illustrated in Figure 3), Gordon and Loeb (2002) calculated an optimal level of cyber security investments. Thus, a company should invest up to 37 % of the expected loss through a cyber attack.[154] This value is calculated on the basis of the assumptions in the model. Nevertheless, the result of the model is important. Investments are only economically rational to a certain level.

5.2 The human factor

In the previous chapter, the problem of human-made threats has only been mentioned and not yet explained. Considering Appendix 1 once again, the following categories of cyber attacks are possible: actions of people, systems and technology failures, failed internal processes and external events.[155] The category actions of people is further subdivided in inadvertent, deliberate and inaction. Of course, attackers are aware of the various possibilities of a cyber attack. In this regard, they often choose unintended security vulnerabilities created by the human factor.[156]

As discussed in chapter 3, the types of cyber attacks were divided and some damage examples assigned. A multiplicity of cyber attacks succeeds only by the

[151] See Sonnenreich et al. (2006), p. 46.
[152] See Sonnenreich et al. (2006), p. 47.
[153] See Gordon and Loeb (2002), pp. 440-452.
[154] See Gordon and Loeb (2002), p. 453.
[155] See Appendix 1: Taxonomy of Cyber Risks.
[156] See Abawajy (2014), p. 237.

unintentional co-operation of the employees, for example, malware that infects the computer by opening email attachments or the Fake President case.

This shows impressively that the biggest danger factor is the workforce of every company. This is in accordance with the results of a study conducted by the Association of Electrical Engineering Electronics Information Technology (VDE). According to this, 77.1 % of the respondents stated that cyber attacks are successful due to the lack of awareness of the employees.[157] Further confirmed the findings of Biener et al. (2015) this origin. Exactly as with the inherited classification of cyber risks, they examined incidents on the origin with regard to actions of people, systems and technical failure, failed internal processes and external events. In the main category cyber Risks, over 90 % were assigned to the subcategory "actions of people".[158]

In defiance of the technological precautions, an essential part arises through ignorance of the user or careless behavior. Examples include shared passwords, opening unknown emails, and clicking on links and email notes.[159]

To reduce these cases, employee awareness of such hazards must be increased. Leoni has done this as a result of the claim, but previous training would help even more to prevent and decrease the probability of a cyber attack.[160] There are several approaches to reduce the human danger by increasing the awareness of employees. Firstly, there are some conventional approaches e.g. posters or newsletters.[161] As newsletter can be an appropriate method to periodically inform employees about current threats, these kinds of teaching by information cannot be checked and therefore, the newsletter can be ignored.[162] A further opportunity is the traditional idea of training by an external security expert.[163] The associated problems are expensive and only temporary. First of all, the expert has to visit the company, resulting in traveling expenses and accordingly, in a costly hourly wage rate. Furthermore, the employees have to attend the presentation, resulting in an interruption of work. Finally, it is usually a unique event which results in a temporary overview of the

[157] See Statista (2019).
[158] See Biener et al. (2015b), p. 139.
[159] See Abawajy (2014), p. 237.
[160] See DerTreasurer (2017), p. 10.
[161] See Abawajy (2014), p. 241.
[162] See Abawajy (2014), p. 241.
[163] See Valentine (2006), p. 18.

current situation. Therefore, a company encounters a steady changing problem with a static solution.[164]

Nowadays, several online approaches are available and various subtypes developed from the opportunity, including e.g. e-mail broadcasting, blogging, game-based models and multimedia.[165] In this regard, it can be seen that online training has a significant impact on employee awareness. A mix of video, text and game-based training, achieves the highest improvement in the perception that the distribution of malware takes place through URLs or emails.[166] With this provision, one addresses a major source of cyber attacks that are difficult to prevent by technological precautions.

5.3 Organizational precautions

This subchapter combines technological precautions with the human factor. As a result, the probability of a cyber attack cannot be entirely eliminated. At the organizational level, hence, two precautions must be taken. On the one hand, measures that reduce the occurrence of damage. Therefore, operating instructions and defining the sphere of competence (e.g. user rights, bank authorization) are measures that support and protect the company and each individual employee. On the other hand, a company needs to define internal processes that allow to minimize the damage in case of an attack. These processes, scope of responsibility and contact person have to be clarified in a crisis management plan.[167] This general advice applies to every possible risk in order to be prepared accordingly. With regard to cyber risks, a more appropriate emergency plan must address the following areas:[168]

- Damage Assessment – a company has to determine quickly what happened and which business line is affected.
- Public Relations – who reports to whom?
- Need for Outside assistance – most of the companies are not specialized in IT systems, data protection law or public relation activities. Therefore, they need an extern expert to support them.

[164] See Valentine (2006), p. 18.
[165] See Abawajy (2014), p. 246.
[166] See Abawajy (2014), p. 246.
[167] See Trautman et al. (2013), p. 110.
[168] See Trautman et al. (2013), p. 110.

- Which source of error enabled the incident?
- Monitoring and adjustments to prevent future attacks of the same kind.

Kulikova et al. (2012) identify various factors affecting the decision of a company if they disclose cyber attacks. On this basis, the importance of clear responsibilities arising from a crisis management plan is analyzed. The first influencing factor is the limitation of damage and prevention. They argued that disclosing an incident helps a company to strengthen the awareness of employees. [169]Afterward, they can assess situations better, reducing the probability of an incident and reducing the damage in case of an incident. Furthermore, regulatory compliance affects disclosure. As mentioned already, the GDPR requires notification. Thus, a decision to omit may result in fines and must be considered in the decision. This entails the resulting costs resulting from data breaches. However, the costs vary depending on the period of publication.[170] Lastly, the reputation of the affected company suffers, in particular, if there is no compliance with the law.

As a result, the identified content of a contingency plan matches the factors that determine the publication of an incident. Furthermore, the crisis plan also addresses the possible costs arising from an attack. These organizational precautions complement the precautions to reduce the probability and determine the following measures.

In particular, the GDPR makes this clear organizational structuring necessary. There were several explanations and examples showing that cyber attacks and personal customer data are linked very closely. Therefore, in case of an incident, it has to be checked which data were affected, what happened to it and how to comply with the notification obligation.

[169] See Kulikova et al. (2012), p. 105.
[170] See Ponemon Institute (2011), p. 4.

5.4 Current Studies

The main problem analyzing cyber risk was the limited available empirical information.[171] Nowadays, the GDPR has increased the transparency of cyber attacks and increased the data sources through the compulsory registration. An occurring cyber attack does not necessarily mean that the incident is also recorded. First of all, the cyber attack has to be detected. The reason why the cyber attack is detected can vary differently. Either the target of a cyber attack detects the incident itself or the organization is informed by the attacker or a connected stakeholder e.g. a credit card processor, IT forensics or a consumer.[172] Afterward, the cyber attack has to be disclosed to appear in the statistics. According to the GDPR, a cyber attack has to be reported to the supervisory authority, if personal data is affected. In this regard, legal regulation has increased the likelihood of a disclosure. This relationship is shown in Figure 4.

Fig. 4: Disclosure of cyber incidents[173]

A further limitation to given data results from the data source. Due to the sensitive issue and reach, no own study was carried out, but public data sources were used. Using a publicly available data set, it is important to consider the backgrounds of the publisher. When analyzing the results, it is therefore considered that insurers and IT security companies might have an evident reason to issue higher numbers.

First of all, the results of the German Federal Office are presented. [174] The following results refer to the year 2018 and enable a current overview of cyber security in Germany. The survey was conducted as part of the Alliance for cyber security. Therefore, it can be assumed that companies which participated have an increased affinity to IT security and the results cannot generally be considered as

[171] See Biener et al. (2015b), p. 133.
[172] See Romanosky (2016), p. 122.
[173] Source: Own representation based on Romanosky (2016), p. 122.
[174] See Federal Office for Information Security (2019b).

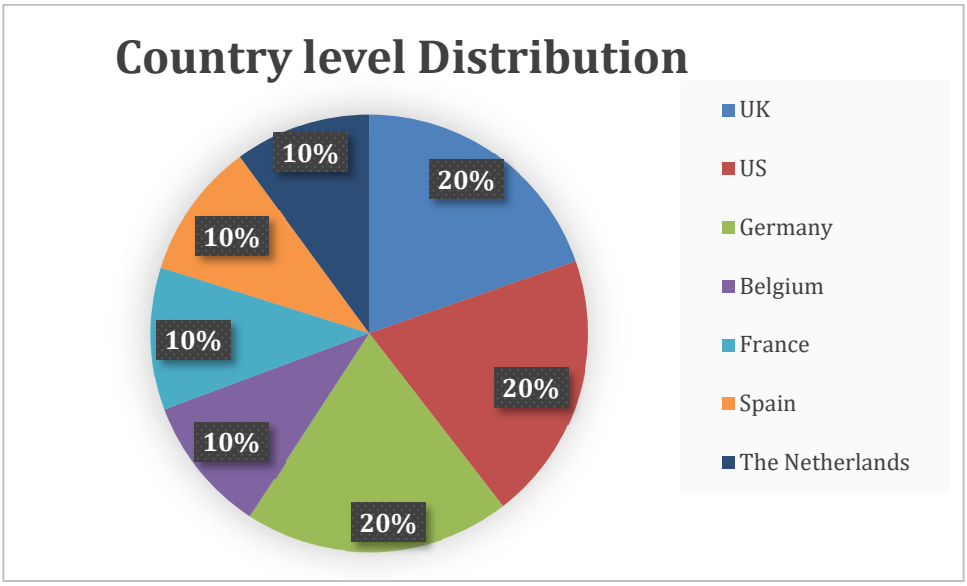
representative for every German company. This assumption is reinforced by the fact that 77 % of respondents were IT security officers, whereby some small companies have not even hired such a position. Nonetheless, it is a good source of data to arrange the opinion of professionals. The results are based on responses from 1,039 participating institutions, of which 57 % were small and medium enterprises with 1 to 249 employees. The remaining 43 % were large companies or institutions with at least 250 employees.

The results form the following opinion: 76 % perceive that cyber attacks have the potential to impact operational processes, 88 % realize digitization is associated with additional cyber risks, 61 % think that cyber security achieves no added value and only 51 % confirm that the business management deals with cyber security.

Furthermore, the survey provides information about the current threat situation: Almost half (43 %) of the large companies were affected by cyber security incidents. For SME this parameter value amounts to 26 %. Moreover, it is notable that 50 % of the attacks were successful and the unreported cyber attacks are not registered in these numbers. According to the survey, the consequences of cyber attacks are enormous. The vast majority (87 %) of the affected companies reported operational failures or interruptions. Almost two thirds (65%) of those affected had costs for the investigation and restoration of the IT systems and 22 % stated to have suffered reputational damage.

In order to obtain an international comparison, the study of the specialty insurer Hiscox is presented below. Forrester Consulting carried out an international survey on behalf of the insurance company Hiscox and summarized the results in the Hiscox Cyber Readiness Report 2019. The results were recorded in an online survey between October 22 and December 7, 2018. In this regard, 5,392 people who where involved in the company's cyber security strategy answered the questions, which enables an assessment of the current situation. Figure 5 shows the country-specific participation.

Fig. 5: Country-specific participation[175]

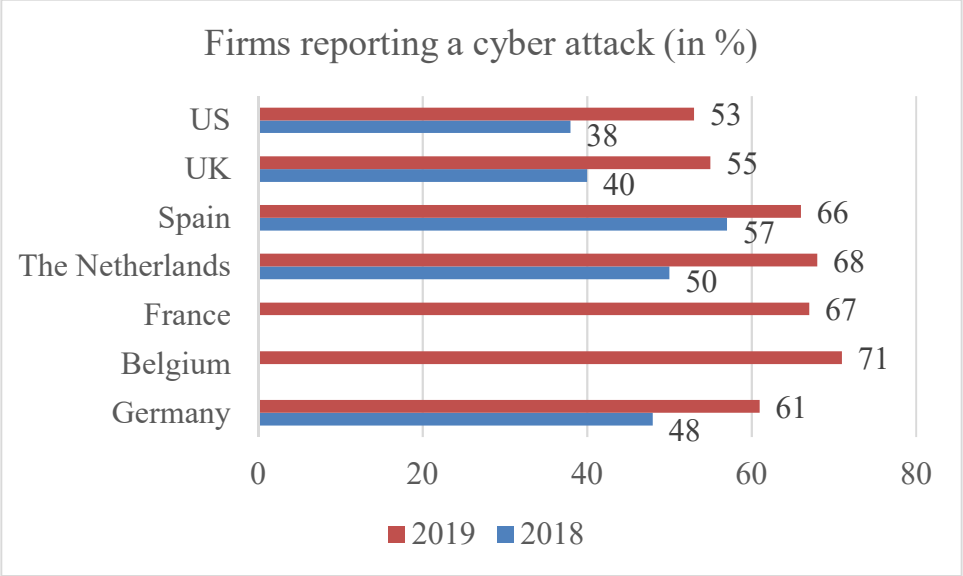


The sample consists of 1,071 companies from the US, 1,060 from the UK, 1,061 from Germany, 546 from Belgium, 567 from France, 543 from Spain and 544 from the Netherlands, and the domestic division of companies can be seen as representative for the respective countries. Therefore, the study provides results of an international consideration for continental Europe, the United Kingdom, and the United States.

One of the key findings of the survey is shown in Figure 6. The proportion of firms, which were affected by a cyber attack, has risen significantly in every country. The proportion is in every country over 50 %, which clearly shows the current and increasing threat.

[175] Source: Own representation based on Hiscox (2019a), p. 4.

Fig. 6: Firms reporting a cyber attack on a county level[176]

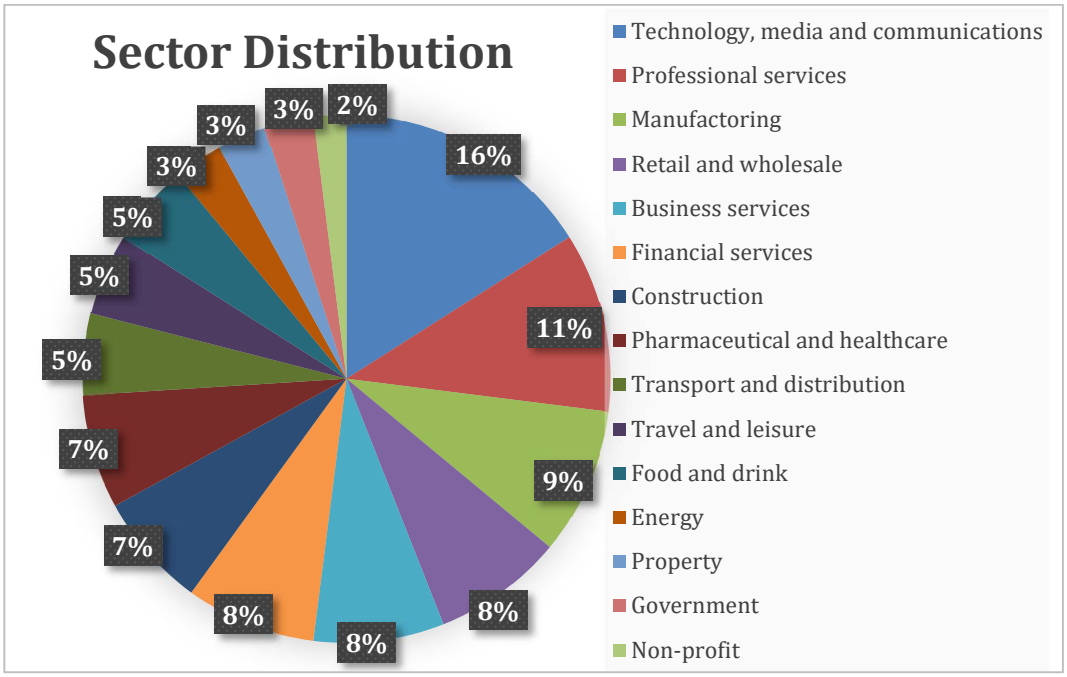


Since the questions and definitions were the same, the descriptive statistics demonstrate a clear increase. In Germany, the proportion increased from 48% to 61%, which corresponds to a relative growth of over 27%.

Regarding the overall sample, cyber attacks are neither a phenomenon of large corporations nor are individual sectors affected, even if certain tendencies are discernible. First of all, 74 % of enterprises, with more than 1,000 employees, suffered from a cyber attack in the last 12-month period. In contrast, small businesses with less than 50 employees are less often affected. However, the severity of 47% represents an immense risk, even for small companies.[177] Looking at the group of SME aggregated, a surge in the last year is noticeable. The fraction rose on average by 59 % compared to the previous report.[178] Figure 7 reveals the corresponding distribution of the sectors.

[176] Source: Own representation based on Hiscox (2019a), p .4.
[177] See Hiscox (2019a), p. 4.
[178] See Hiscox (2019a), p. 4.

Fig. 7: Sector of the participating companies[179]



The illustration only shows that various sectors were surveyed, which obtain a holistic picture of the economic situation. Hence, the allocation of samples shows that the results range over a multitude of different sectors. As a result, the progress of increasing cyber attacks extends to every measured sector and demonstrates that cyber attacks can affect any industry.[180] Nevertheless, due to empirical data, some industries are more often affected. In 2018, technology, media, and communications companies were the most affected as 72 % of the respective companies have stated an attack. The second-highest attack rate had government entities with 71% and subsequently, 67 % of the financial sector was affected.[181]

Another illustration provides the results of the IBM Report, which represents all attacks relative to the industry.

[179] Source: Own representation based on Hiscox (2019a), p. 16.
[180] See Hiscox (2019a), p. 5.
[181] See Hiscox (2019a), p. 5.

Table 4: Relative assignment of cyber attacks[182]

Industry	Proportion
Finance and Insurance	19 %
Transportation	13 %
Professional Services	12 %
Retail	11 %
Manufacturing	10%
Media	8 %
Government	8 %
Healthcare	6 %
Education	6 %
Energy	6 %

Table 4 shows the sector distribution of cyber attacks. The advantage of this representation is its relative relationship to the totality of cyber attacks. Accordingly, 19 % of global cyber attacks have affected the financial sector. However, the totality of attacks is shared by a variety of other industries. These results confirm that cyber attacks affect every industry.

In summary, cyber attacks have increased worldwide. Big companies are even more affected than small companies. Nevertheless, the threat can be considered very high, with 61% of international companies reporting a cyber attack. These attacks are spread across all industries, with an increased likelihood for financial companies. Looking more closely at Germany, the figures of the affected companies vary. KMPG published a report whichs shows that in the last two years 39% of the German enterprises were affected. [183] In addition to the results already presented, it can be said that cyber attacks pose a danger that can affect any business.

Further findings demonstrate that not only the frequency of cyberattacks increases, but also the associated costs for the companies. Looking at the global mean costs, they have increased within the last year by 61 %.[184] Global mean costs of companies

[182] See IBM (2019), p. 16.
[183] See KPMG (2019), p. 11.
[184] See Hiscox (2019a), p. 6.

due to cyber attacks have increased to 369.000 $. Furthermore, the mean impact of a single incident has multiplied, too.[185]

6. Insurability of cyber risks

6.1 Cyber Insurance – Definition and scope of benefits

Insurances have always been part of risk management, as an entrepreneur can influence which existing risks they are willing to bear and which they give to an external third party against the payment of a security premium. The first ideas for insurance of digital risks were already mentioned in the scientific literature in 1994.[186] The fact that a company incurs costs and losses when the IT system fails is not new. Thus, the entrepreneurs are aware that when for example, the required hardware is burned by a fire or the server room is destroyed, it causes the company significant losses.[187] On the one hand, the technical capabilities have increased the risk of a cyber attack. On the other hand, the consequences of a cyber attack have explicitly changed. These technological and judicial changes result in potential danger for companies, where classical insurance products have no coverage.[188] With cyber insurance, a company can hedge potential losses from a cyber attack.[189] The German insurance Provinzial describes on its homepage the purpose of cyber insurance as protection against the consequences of hacker attacks on your IT systems and other digital risks.[190] Compared to this more general descriptions, the American International Group, Inc. (AIG) directly refers to cyber risks. Hence, their cyber insurance covers losses for data protection and network security breaches in the use of computer systems and the internet.[191] The core of the definition remains the same, and a detailed comparison of the available insurance policies is elaborated in chapter 7.3.

[185] See Hiscox (2019a), p. 6.
[186] See Lai et al. (1994), p. 171.
[187] See Gordon et al. (2003), p. 82.
[188] See Gordon et al. (2003), p. 81.
[189] See Gordon et al. (2003), p. 81.
[190] See Provinzial (2019).
[191] See AIG (2019).

6.2 Problems and needs

So far, cyber risk has been identified as a rapidly growing threat, which must definitely be considered in complete risk management. Even current studies of the last years show an ever-increasing danger. Anyway, there are some problems associated with cyber risks and the potential implementation of risk management instruments. The main problems are comparable to most other insurance contracts: Adverse selection and moral hazard. Adverse selection describes the fact that more vulnerable companies rather seek for insurance than safer companies.[192] Moral hazard, on the other hand, illustrates a problem after signing the contract. According to this, companies have less incentive to upgrade IT security after risk transfer has taken place.[193] Moral hazard and adverse selection are not further discussed here, as they are not a peculiarity of cyber risks and need to be assessed by insurance companies. When deciding whether companies take out insurance, these factors are not crucial. Measures taken by insurers are examined as part of the market analysis.

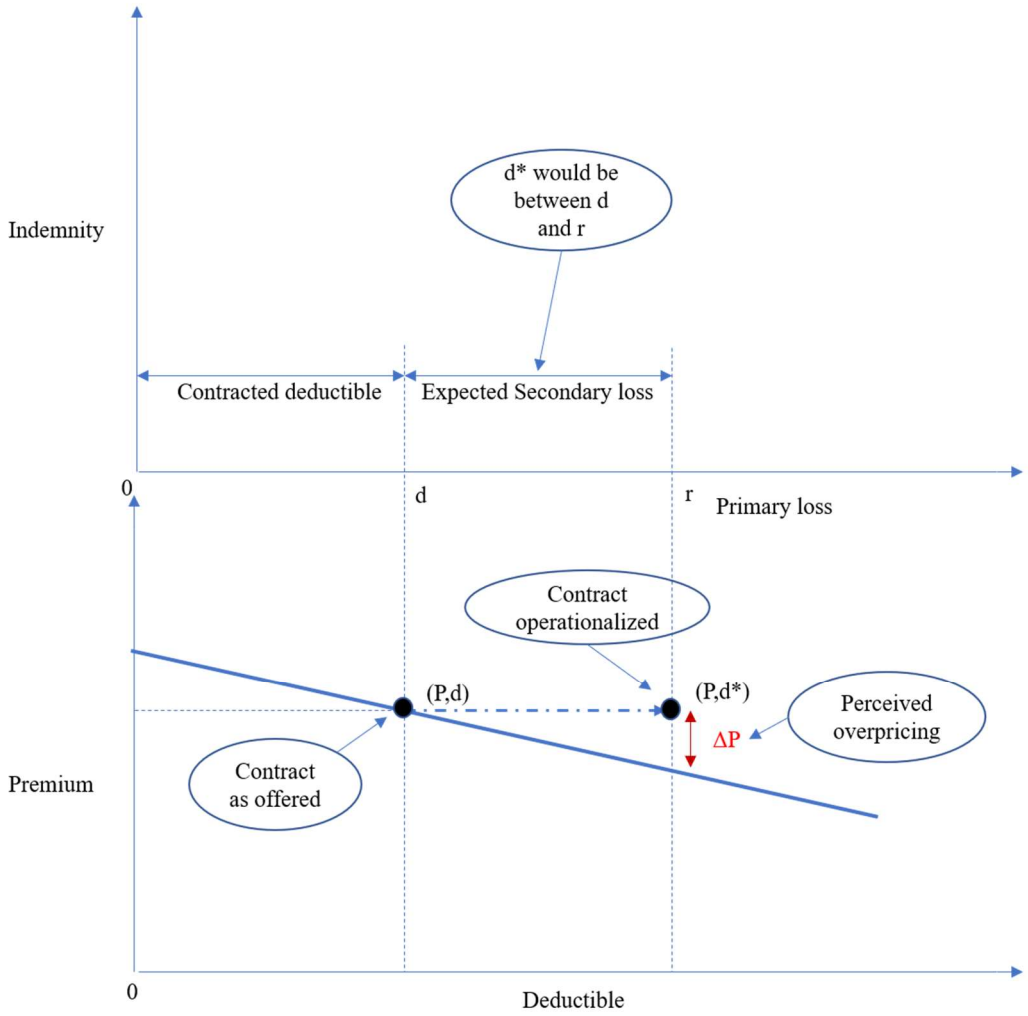
As these problems are not really new, the main difficulty is the pricing of cyber insurance contracts. Insurance premiums are determined on the basis of empirical claims. Other insurance lines, like automobile insurance, have little changing factors. Therefore, the empirical data can be considered as representative of future damage. Cyber attacks, however, are associated with two novel problems. For one thing, companies have not been willing to make the incidents public, resulting in a small amount of data.[194] Furthermore, other factors continue to change steadily, making it difficult to provide up-to-date security. Attack possibilities increase, for example, through the development of the Internet of Things. These factors, in combination with a rather new line of the insurance business, initially lead to inflated insurance premiums.[195]

Bandyopadhyay et al. (2009) developed a theoretical model, that explains the overpricing of cyber insurance contracts.[196] Essential components of this model are the annual premium P, the deductible d, the primary loss A and the secondary loss B.

[192] See Gordon et al. (2003), p. 82.
[193] See Gordon et al. (2003), p. 82.
[194] See Gordon et al. (2003), p. 82.
[195] See Bandyopadhyay et al. (2009), p.68.
[196] See Bandyopadhyay et al. (2009), pp. 69f.

The probability p is assigned with the respective index. Furthermore, introduced cost types primary and secondary, and the characteristics of the incident, so whether it is a systematic or symptomatic and a private or a public incident are important. Cyber insurances are basically built like classic insurances, i.e. the policyholder pays in advance the insurance premium P. If an insured event occurs, the insurer pays the insured losses minus the agreed deductible. The premium and the deductible have an inverse relationship, meaning a higher deductible reduces the premium. The model is illustrated in Figure 8. An important limitation of subsequent description is the assumption that no regulatory framework affects the disclosure of data breaches. Therefore, the model is evaluated afterward.

Fig. 8: Overpricing of a cyber insurance contract[197]



As already mentioned, a cyber insurance contract is connected with a contracted deductible d. The basic consideration is that different types of cyber attacks have

[197] Source: Own representation based on Bandyopadhyay et al. (2009), p. 71.

different effects. A cyber attack leads to primary losses, resulting directly in every successful attack, and secondary losses, resulting only in public incidents or private symptomatic breaches. If the company has taken out a cyber insurance policy, then it can report the losses to the insurance company. Crucial for further consideration is the decision of disclosing a symptomatic breach. If the affected company does not disclose the breach but claims the primary losses, the company insurance company pays existing losses. Claiming a loss to an insurance company involves extern partners, which increases the probability of secondary losses. Hence, the other alternative is not claiming the primary losses and definitely avoid the secondary losses.

The model assumes an optimal amount of deductible d*, which determines an optimal amount of insurance premium P*.

If a company claims the primary losses to the insurance company, there is a probability p_B that secondary losses B emerges from claiming. This interrelation enables the following conclusion: Claiming a symptomatic breach results in the contracted deductible d and the expected secondary loss $p_B * B$. This sum of costs is marked with the small letter r. As a result, a targeted company will not claim losses from a cyber attack, if they are smaller than $r = d + p_B * B$. Thus, changing the point on the x-axes and the offered deductible d does not equate to the actual participation. Finally, the realized deductible d* = r would correspond to a reduced insurance premium. Indeed, this results from the market mechanism and is not arranged with the insurance company. If IT managers weigh up this matter, they perceive cyber insurances as too expensive compared to the realized deductible.[198]

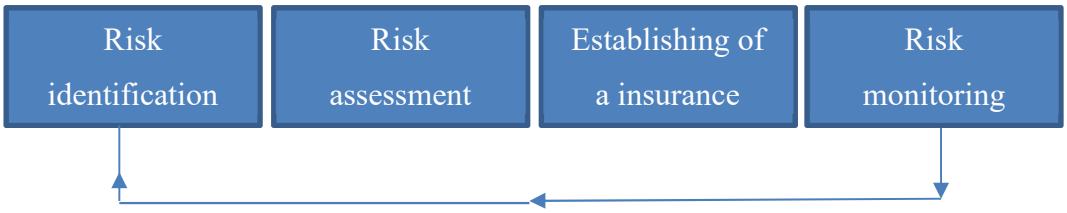
6.3 Insurances in Cyber Risk Management

Cyber threats are a very abstract danger. Therefore, it is essential to reduce the risk, minimize the probability of being attacked and secure the rest probability of actual damage. As early as 2003, Gordon et al. (2003) identified cyber insurances as an integral part of the IT security risk.[199] Accordingly, the basic principle of risk management also applies here: Reduce the existing risk to an acceptable level. To achieve this, companies should use a two-step approach. First, software and

[198] See Bandyopadhyay et al. (2009), p. 71.
[199] See Gordon et al. (2003), p. 84.

hardware should be improved to enhance technical protection against cyber attacks. In the ever-technological world, even with the best security systems, you cannot achieve 100% protection. The introduced studies in chapter 5.4 demonstrate this explicitly. The second step recommends the conclusion of a cyber insurance policy. Gordon et al. (2003) describe the insurance as a "management tool for reducing the risk of financial losses associated with Internet-related breaches"[200]. Applying the traditional risk management process from chapter 2.1 to risk transfer by insurance, the steps change to a customized process, as shown in Figure 9.

Fig. 9: Risk transfer process via insurance[201]



Step 1 and 2 remain unchanged from the specific risk as already described. Due to the enormous importance that has been identified in the risk identification and evaluation, in step 3 a suitable insurance is taken out to minimize the residual risk. Depending on the company and the needs, a suitable cover is agreed that affects the annual premium. As the risks in the cyber sector change dynamically, monitoring is of enormous importance.

Today the insurances include far more than the first policies. The existing opportunities will be compared in the next chapter.

[200] Gordon et al. (2003), p. 84.
[201] Source: Own representation based on Hallikas et al. (2004), p. 52 and Marotta et al. (2017), p. 41.

7. German Market analysis of available insurances

7.1 Available cyber insurance tariffs in Germany

After defining the cyber insurance product in chapter 4.1, the available insurance companies and the corresponding tariffs are compared and analyzed.
The current market situation is still growing. Nowadays 29 insurance companies offer a variety of tariffs and combinations.[202]

Table 5: Supply of the German insurance market respective cyber insurances[203]

Insurance company	Tariff
American International Group AIG Europe S.A.	"CyberEdge online 3.0", as of 08.2018
Allianz SE	"Cyber Schutz", "Cyber-Erpressung", "Fehlerhafte Bedienung", "Datenmanipulation / Telefonmehrkosten", "Externe Dienstleister", as of 09.2018
ARAG SE	"Busniess Aktiv CyberSchutz", "Business Aktiv CyberSchutz PLUS", as of 01.2017
AXA S.A.	"ByteProtect Kompakt", "Baustein F Internet-Betrug", "Technische Störungen", as of 05.2018
Basler Versicherung AG	"Cyber-Police mit Betriebsunterbrechung wegen Ausfall des Dienstleisters und Sublimit-Anhebung", as of 01.2019
Barmenia Allgemeine Versicherungs-AG	"Gewerbe-Cyberrisiko-Versicherung", as of 01.2019
Versicherungskammer Bayern	"CyberSchutz 2017 mit Ertragsausfallversicherung", as of 03.2018
BGV-Versicherung AG	"BGVFIRM Cyber Versicherung"

[202] See GDV (2019) and Franke and Bornberg (2019).
[203] Source: Own representation based on GDV (2019) and Franke and Bornberg (2019).

Chubb European Group SE	“Cyber Enterprise Risk Management“
CNA Insurance Company (Europe) S.A.	“Netprotect®“
Condor Versicherungen	“CyberRiskPolice“, as of 01.2017
DUAL Deutschland GmbH	“Cyber Defence“, as of 01.2015
ERGO Versicherung AG	“Cyber-Versicherung“, as of 01.2018
Gothaer Group	“Cyber-Versicherung für Gewerbekunden“ and “Erhöhung der Sublimits auf 20% der Versicherungssumme“, as of 10.2018
GVV-Kommunalversicherung VVaG	“Cyber-Versicherung für Kommunen und kommunale Unternehmen“
HDI Global SE	“Cyberversicherung für Firmen und Freie Berufe“, “Leistungs-Update-Garantie“, “Internet-Diebstahl“, “Cyber-Spionage“, and “Betriebsunterbrechung durch Cloud-Ausfall“, as of 10.2018
Helvetia Schweizerische Versicherungsgesellschaft AG	“Business Cyber“, as of 01.2018
HISCOX S.A.	“CyberClear“, “Cyber-Betrug”, “Cyber-Betriebsunterbrechung bei Technischen Problemen“ and “Cyber-Betriebsunterbrechung durch Cloud-Ausfall“, as of 03.2019
LVM Landwirtschaftlicher Versicherungsverein Münster a.G.	“Sach-Gewerbeversicherung - Cyber-Risikoversicherung“, as of 10.2018
Markel International Insurance Company Limited	“Markel Pro Cyber“, “Cyber-Forderung“, “Cyber-Zahlungsmittel“, “Cyber-Vertrauensschaden“, and „Cyber-Haftpflicht“, as of 01.2018

Provinzial AG	"Cyber-Versicherung mit Bausteinen Haftpflicht, Eigen-, Vertrauensschaden, Ertragsausfall", as of 04.2019
QBE Insurance (Europe) Limited	"Cyber-Response", as of 01.2017
R+V Versicherung AG	"CyberRisk-Versicherung", as of 09.2017
SIGNAL IDUNA Allgemeine Versicherung AG	"Cyberrisiko-Versicherung", as of 10.2017
SV Versicherung AG	"SV CyberSchutz", as of 08.2017
VGH Landschaftliche Brandkasse Hannover	"CyberSchutz für Firmenkunden und Landwirte", "Cyber Rechtsschutz", "Cyber Vertrauensschäden", "Cyber Betriebsunterbrechung", as of 02.2018
VHV Allgemeine Versicherung AG	"CYBERPROTECT", as of 02.2018
Württembergische Versicherung AG	"Cyber-Police", as of 01.2018
XL Insurance Company SE	"Cyberschaden-Versicherung", extension of cover: "Betriebsunterbrechung - externe IT-Dienstleister", as of 01.2018

Table 5 presents the available tariffs of cyber insurance in Germany. The summary was compiled on the basis of own research, the market research by Franke and Bornberg[204] and an overview by the German Insurance Association[205] (GDV). Tariffs, which are listed on the GDV but cannot be found on the specific insurance website, are extinguished in the table. Furthermore, the list contains the insurer with the list of partially optional components of cyber insurance. In the column of tariffs, the German designations were used and the date of the respective insurance terms and conditions added. In some cases, this date is missing. There, the tariff is available online, but the insurance terms and conditions were not detectable.

[204] See Franke and Bornberg (2019).
[205] See GDV (2019).

7.2 Assessment of available tariffs and rating

Franke and Bornberg, founded in 1994, is an independent German company that compares insurance products and insurance companies critically and consumer-oriented with a specialization for SME.[206] In October 2018, they published a press release presenting the results of a recent cyber insurance market analysis.[207] Sources include only legally binding documents, e.g. printed insurance terms, mandatory consumer information, application forms, insurance policies, and annual reports.[208] The analysis examined commercial cyber policies in the German market. Included were 35 insurance tariffs from 28 providers. All insurance tariffs have been rated according to the internal rating criteria for cyber insurances.[209] There was a detailed evaluation of individual subgroups. The following categories were examined: General categories of insurance benefits, exclusions, business interruption, third-party claims, e-payment, increased risk, IT forensics and consulting, costs resulting from a breach of privacy, crisis and reputation management, multiple insurance contracts, pre-insurance claims, representatives, penalties, insured risks, insured IT systems, insured persons and companies, insured event, insurance contract, trust damage and the restoration of IT systems. All categories were rated according to their sub-items and their weighting to finally receive an overall rating. In order to take account of important contract contents, the sub-items were weighted into the overall rating. Franke and Bornberg assess the following as essential: loss of revenue & additional costs, interruption of business due to cloud failure, third party liability assumed by exemption, contractual liability, infringement of personal rights, geographic sphere of influence, contract of risk aggravation, notification obligations in data protection breaches, crisis management, clarity of wording obligations, definition of the insured risks, definition of the insured IT systems as well as the restrictions on the restoration of the IT systems.[210] Table 6 shows the general classification of the rating classes of Franke and Bornberg based on the percentages achieved.

[206] See Franke and Bornberg (2018a), p.6.
[207] See Franke and Bornberg (2018a).
[208] See Franke and Bornberg (2018b), p. 5.
[209] See Franke and Bornberg (2019).
[210] See Franke and Bornberg (2018a), p. 4.

Table 6: Rating classification according to Franke and Bornberg[211]

Percentages	FFF-score	Written score	School grade
≥ 85 %	FFF+	Excellent	0,5
≥ 75 %	FFF	Very good	0,6 until 1,5
≥ 65 %	FF+	Good	1,6 until 2,5
≥ 55 %	FF	Satisfactory	2,6 until 3,5
≥ 45 %	F+	Sufficient	3,6 until 4,5
≥ 35 %	F	Poor	4,6 until 5,5
< 35 %	F-	Deficient	6,0

The current assessment of available cyber insurances, according to the rating classification of Franke and Bornberg, is shown in Figure 10. The decisive factor for this classification is the database of Franke and Bornberg retrieved on July 2019 and their current classification based on available tariffs.

Fig. 10: Classification of current available cyber insurance tariffs[212]

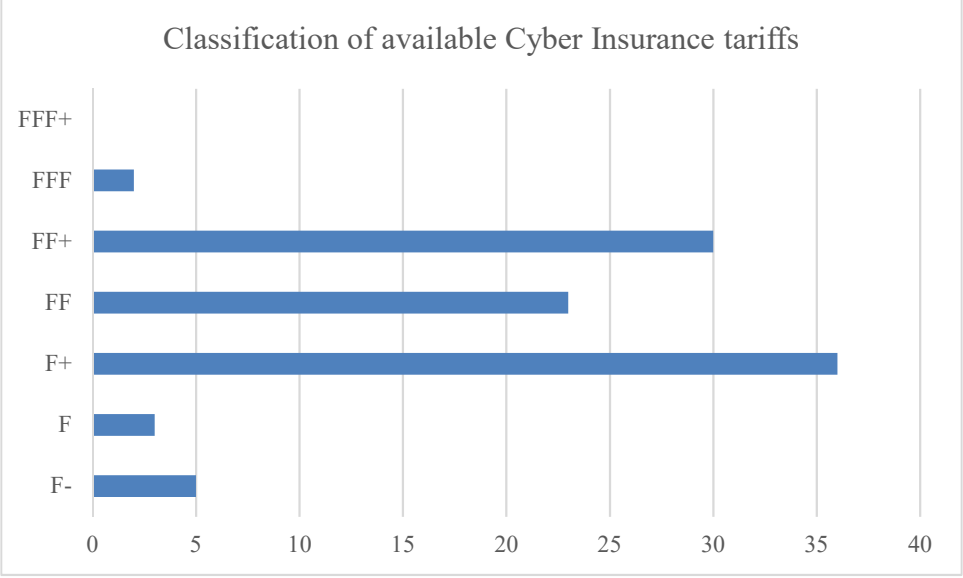


Figure 10 shows that the best score FFF+ is not yet achieved by existing cyber insurances. Nevertheless, two tariffs receive a score of 1,5. This corresponds to a very good covered exposure with an overall percentage of at least 75 %.

[211] See Franke and Bornberg (2018b), p. 8.
[212] See Franke and Bornberg (2019).

Comparing this classification with the published evaluations in the 2018 press release, it becomes evident that cyber insurances are constantly evolving. A year earlier, no insurance tariff reached FFF rating and only 11.85% achieved FF + rating.[213] In 2019, 30 out of 99 tariffs were evaluated in this category, which represents a percentage of 30.30 %. The increase in the FF+ class refers to 1,845 basis points. Furthermore, the development shows that not only other tariffs are getting better, but also fewer tariffs are being grouped into the worst group. Therefore, the risk of inadequate coverage has slightly declined. Nevertheless, qualitative differences between insurers and insurance tariffs still remain. For informational reasons and to appreciate the good development, Table 7 contains the insurance companies and tariffs that have reached the FFF and FF + ratings. In the previous enumeration of the available cyber insurances, the list was sorted alphabetically. In the present case the ranking is arranged depending on the assessment. The number deviates from the number of tariffs mentioned above because in turn the different optional building blocks were combined in one row and awarded the best-achieved ranking. Therefore, the maximum number usually stands for the combination of all options.

Table 7: Best rated cyber insurances 07/2019[214]

Insurance company	tariff	FFF-Score
Provinzial AG	"Cyber-Versicherung mit Bausteinen Haftpflicht, Eigen-, Vertrauensschaden, Ertragsausfall", as of 04.2019	FFF
American International Group AIG Europe S.A.	"CyberEdge online 3.0", as of 08.2018	FF+
HISCOX S.A.	"CyberClear", "Cyber-Betrug", "Cyber-Betriebsunterbrechung bei Technischen Problemen" and "Cyber-Betriebsunterbrechung durch Cloud-Ausfall", as of 03.2019	FF+

[213] See Franke and Bornberg (2018).
[214] See Franke and Bornberg (2019).

Basler Versicherung AG	"Cyber-Police mit Betriebsunterbrechung wegen Ausfall des Dienstleisters und Sublimit-Anhebung", as of 01.2019	FF+
HDI Global SE	"Cyberversicherung für Firmen und Freie Berufe", "Leistungs-Update-Garantie", "Internet-Diebstahl", "Cyber-Spionage", and "Betriebsunterbrechung durch Cloud-Ausfall", as of 10.2018	FF+
Gothaer Group	"Cyber-Versicherung für Gewerbekunden" and "Erhöhung der Sublimits auf 20% der Versicherungssumme", as of 10.2018	FF+
Markel International Insurance Company Limited	"Markel Pro Cyber", "Cyber-Forderung", "Cyber-Zahlungsmittel", "Cyber-Vertrauensschaden", and „Cyber-Haftpflicht", as of 01.2018	FF+

7.3 Selected insurance benefits in comparison

So far, the threat situation has been discussed intensively and offered insurance tariffs receive a good to a very good overall rating. Even so, insurances in cyber risk management do not seem to have become a standard instrument. Therefore, selected tariffs will be examined more closely to identify differences, strengths, and weaknesses. The comparison includes mentioned tariffs from Gothaer, HDI, Hiscox, and Markel with FF+ rating[215] and an exemplary tariff rated F+ (AXA ByteProtect[216]). The selection was chosen based on the public availability of the information and the previous findings of Franke and Bornberg[217]. Subsequent analysis should be understood as a point-in-time analysis. Therefore, the results may vary over time.

[215] See Table 7.
[216] See Franke and Bornberg (2019).
[217] See Franke and Bornberg (2019).

Based on the problems and previous knowledge of the thesis, the comparison includes the contingency risk, liability limits, sum insured, insurable dangers, and technological underwriting. A detailed analysis can be found in Appendix 2.[218]

The contingency risks are rather comparable and include network security breaches, operator error, data infringement, cyber extortion, and infringement by advertising and marketing. The common sources of damage like hacking, DDoS-attacks or malware are covered by every insurance. Also noteworthy is the coverage of random attacks and planned attacks by employees.
Regarding liability, the contracted sum insured is decisive and only a few important aspects are excluded in some tariffs, e.g. fines from abroad in the AXA tariff. Depending on the insurance, technological precautions are required, as explained in chapter 5.1.1. Possible required precautions are state of the art, physical access controls, firewall, and antivirus software.
What makes cyber insurance special is not only the financial damage, but the product is optimally complemented by additional services. Each closely considered tariff has at least the possibility of an employee awareness training and the creation of a crisis management plan. The second crucial component is the assistance service in case of damage. The insured company benefits from a permanently available hotline and expert support, even if there is just a suspicion of a cyber attack. Insurers have access to experts in legal and technological matters due to greater scalability.

7.4 Critical appraisal and the recommended action

This chapter assesses the issues and insurance tariffs from the perspective of market demand. As a result, only the overpricing of the insurance premium and the lack of coverage are relevant in cyber risk management. In chapter 6.2, the model of Bandyopadhyay et al. (2009) was presented, which explains why cyber insurance is perceived as overpriced. This problem can be resolved if the extent of coverage of cyber insurances changes. As cyber attacks are connected with primary and secondary losses, an appropriate hedging instrument should include constituents' parts addressing both types of losses.[219]

[218] See Appendix 2: A comparison of selected insurance tariffs.
[219] See Bandyopadhya et al. (2009), p. 73.

Considering the associated assumptions, as well as the current market conditions, it becomes clear that it is no longer appropriate for the German insurance market. First, the General Data Protection Regulation forces companies to report a data breach within 72 hours, which significantly increases the likelihood of secondary losses and legally excludes private attacks. Furthermore, meanwhile the insurance products have adapted to this development.
One development is that good tariffs already cover a fairly comprehensive origin of cyber attacks. A further development consists in the extending of the overall package to address every consequential damage due to a cyber attack. These options are in line with the identified sources and consequences of cyber attacks. The human factor is a source, which has to be updated constantly, analogous to the technological side. Therefore, it is important to repeat awareness training for example in a yearly period. The restriction to six months is therefore negative for the AXA tariff. Insurance companies tried to create a product, which helps entrepreneurs to reduce consequential costs, e.g. due to public relation consulting. Reputation damage was one of the significant damages, resulting from an attack. Insurance will not compensate the company for the resulting reputation damage but the access to PR consultants and lawyers, who are familiar with cyber attacks, supports the company subsequently. Extending insurance coverage thus can minimize consequential damage. So, the development of cyber insurance is positive and can support companies in the digitalization.

As an intermediate conclusion can be stated that cyber insurance is especially meaningful for SME because they get access to experts and can increase their knowledge. In addition to financial protection, they can reduce the likelihood of an attack.
Beyond that, large companies and enterprises require in particular the financial hedge because the associated costs increase significantly with company sales and stored data.

Hence, the numbers, facts and their development clearly speaks for the conclusion of cyber insurance. Looking at the current coverage rate, this development seems to go on. According to the Hiscox Cyber Readiness Report 2019, 41 % of the companies included in the sample, have adopted cyber insurance, 30 % are going to adopt insurance during the next twelve months, 26 % are not planning to adopt an

insurance and 3 % don't really know what cyber insurance is.[220] For German companies, the number of firms who implemented cyber insurance is even larger. Referring to the survey of the Alliance for cyber security, 61 % have adopted cyber insurance.[221] There it is important to be aware of the fact, that the survey was answered by companies that are familiar with the risk. We cannot adopt this number as an universally valid example. Nevertheless, we can see that a bigger part of companies that have dealt with the risk has already adopted insurance. I assume that the real number of companies, having cyber insurance is noticeably smaller. The actual value varies. Depending on the source, the coverage rate is between 13 % and 61 %.[222] The idea is supported by the recent study by consulting firm KPMG, which noted a current coverage of 27 %.[223] Another 28 % said that they are about to take out insurance, whereas 31% did not know that such insurance exists.[224] This shows impressively that there is still a great demand untapped and insurance companies have to increase the communication.

Finally, it becomes apparent that companies that deal with the risk tend to take out insurance. One the one hand, I can deduce from the behavior that implementing cyber insurance is a recommendable action. On the other hand, the developments in the insurance market are not finished yet. The German cyber insurance market offers an increasing number of insurance companies and tariffs. As the increasing number will continue to drive this positive development in the insurance business, I recommend to select one of the top-rated tariffs and review this choice annually.

[220] See Hiscox (2019a), p. 14.
[221] See Federal Office for Information Security (2019b), p. 19.
[222] See Gothaer (2019), p. 2.
[223] See KPMG (2019), p. 55.
[224] See KPMG (2019), p. 55.

8. Cyber Risk Management – a constant process

8.1 Reassessment of the risk situation

In an increasingly digital landscape, cyber attacks are the dangers with a clearly above-average probability and above-average damage.[225] Management needs to be aware of the danger and evaluate the impact on their own business. On the one hand, in a risk management process, the probability of an attack must be reduced, and on the other, the extent of an attack should be reduced as much as possible.

Due to the General Data Protection Regulation and the interrelation of customer data and cyber attacks, companies are threatened with severe penalties that can be incurred through direct damage control as well as through consequential damage.

Because every business can be affected, a clear response plan needs to be defined which clarifies responsibilities.

In Chapter 2.1, I introduced the classic risk management process in a structured way. The risk must be identified, assessed, risk management actions have to be discussed and potentially implemented, and finally monitored.[226] Applying this approach to the cyber world and the corresponding risks, the process becomes even more precise. Firstly, the potential danger will grow steadily due to the already discussed input factors. The studies in chapter 5.4 represent an industry-independent development with an increasing probability of incidents and increasing associated costs. Thus, a company has to decide for itself how much their company depends on the digital business processes but cannot look at it only one-sidedly due to the GDPR. On the contrary, the scope of cyber risks is not limited to the corporate building. Regarding the data processing, controller and processors are jointly and severally liable for breach of the obligations.[227]

Even precautions like software and hardware are bypassed by skilled hackers. Basically, technologies like anti-virus programs or virus scanners work backward and only react to already known actions and actions of the hackers.[228] As early as 2005, Gordon et al. identified that 97 % of companies own firewalls, 96 % have anti-virus

[225] See chapter 2.5.1 for a detailed analysis.
[226] See Hallikas et al. (2004), p. 52.
[227] In chapter 4.3 is a more detailed analysis of the GDPR and the interconnection with cyber attacks.
[228] See Bandyopadhya et al. (2009), p. 68.

software and 72 % use intrusion detection systems.[229] Nevertheless, cyber attacks are no rarity. This fact leads to the conclusion that cyber risks cannot be completely eliminated by utilizing technologies. Thus, a complete cyber risk management process cannot stop here because a company always have to consider the residual risk. Secondly, the specific cyber risk has to be assessed. After the uncertainty of whether the company is affected by the dangers of cyberspace, can only be confirmed, the estimation of the individual risk is more complicated. As already described, a successful cyber attack can have several effects. Therefore, not only the primary costs are important, but the total impact including secondary costs must be considered.[230] Bringing the theory of primary and secondary costs in connection with the possible cost resulting due to a successful cyber attacks, a firm faces many different forms of costs, e.g. costs due to business failure, costs of IT-recovery and IT-forensic, costs of data recovery, notifications cost, blackmail and manumission payment, monetary fine and contract penalty and finally a reputational damage.
Therefore, the overall assessment should be decisive for the later chosen instruments. In particular, since bearing this kind or risk enables only small or no additional return for companies.

8.2 Adaptation of security measures

"Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies […]."[231]

IDC's definition of cyber security reveals the fact that cyber attacks cannot be handled easily. As discussed in chapter 3, the value of the data continues to increase and the storage of personal data is subject to GDPR. In this regard, data storage and cyber attacks are closely related and cannot be considered separately. This is also shown by the fact that in the case of an attack often personal data is encrypted as past examples of damage in chapter 4.3 and current studies in Chapter 5.4 show.
Therefore, the choice of suitable risk management instrument has to be applied to specific circumstances. Basically, a company has to consider every risk and has to decide whether the company bears the risk itself, reduces it by risk management

[229] See Gordon et al. (2005), p. 11.
[230] See Bandyopadhya et al. (2009), p. 70.
[231] International Telecommunication Union (2008), p. 2.

instruments, or transfers it to a third party.[232] Applying this to cyber risks, the strategies of a firm will be explained in more detail afterward.
Since cyber risks are a complex problem, the concept of a complete hedge includes a combination of every instrument. At least the risk manager should consider all the options and weigh the individual decisions.

Step one of the decision-making process starts with the reduction of the risk factor. This succeeds in cyberspace in particular via suitable software and hardware to achieve a minimum level of technical precautions. With firewalls, network intrusion detection systems and anti-virus software a company can reduce the probability. Even if such software protects the company only against known attacks. Regularly updates guarantee the current state, as the attacks are evolving too. A further technological approach to reducing the overall risk are back-ups in a small-time interval. Back-ups significantly prevent loss and ensure a quick resumption of business activity. [233] Consequently, costs of IT-recovery and costs of data recovery can be reduced.
As with any business investment, it should be economically viable to act in the interests of stakeholders. Therefore, a company must always weigh what the investment costs are and what impact this has on risk reduction. Furthermore, the most common sources of error must be reduced and made known in the company e.g. reckless actions by employees. Taking a closer look at the types of cyber attacks, over 90 % are actions by people. These include for example hacking attacks, physical information thefts, human failures, and data manipulation.[234] Even if a firm can protect itself against attacks from external ones by technical arrangements, unintentional actions of own employees are still a main source of damage. Accordingly, it can be stated that cyber risks can happen due to different ways and the risk must be taken multidimensionally. Technical arrangements, clear organizational procedures, and staff awareness training were identified as components of risk management that reduce the probability of occurrence and the resulting damage. Risk managers have to be aware of the human factor and ensure regular training to increase cyber security awareness of every employee. Because the strongest chain is only as

[232] See Hallikas et al. (2004), p. 54.
[233] See Siegel et al. (2002), p. 48.
[234] See Biener et al. (2015b), p. 139.

strong as its weakest link. In this regard, it was found that employees recognize better dangerous situations through suitable online training.[235]

8.3 The decision on risk transfer

After a company has identified the sources of error and reduced them with appropriate measures, the second step includes the risk transfer to a third party. This step should be carried out in a complete process, as a company can not fully protect itself from the dangers and technical precautions are no longer economical beyond a certain level.[236] In reality, this is possible with cyber insurance. Available tariffs are getting better every year because of the market entry of other insurance companies or an adjustment of coverage schemes to meet demand. Current tariffs, evaluated with FF+ or better, offer more than pure financial security. Especially for small companies, the additional services of prevention helps the manager to reduce risk and the additional services of assistance help companies to comply with structured processes in the event of damage.

When choosing the sum insured, companies can orientate themselves on sales, since in particular the sales and the stored data were identified as central drivers of the primary costs.[237] Considering the market share of companies having cyber insurance, this number varies a lot. As the real number might be much lower, the Alliance for cyber security reported it to be 61 %. It is less important if the value is correct or if it can be considered representative of Germany, but the fact that companies that deal in the context of IT security with cyber risks, tend to take out insurance.

Because every business is faced with cyber risks, additional insurance may make sense. In this regard, companies should assess their own risk profile. If entrepreneurs already have their problems there, insurance is recommended. First, because by weighing the different tariffs, companies strengthen their awareness and self-protection against cyber risks.[238] By means of technical acceptance criteria, insurance companies ensure that a required level of IT security is in place. Furthermore,

---

[235] See Abawajy (2014), p. 245.
[236] See chapter 5.1.2.
[237] Source: Own representation based on Romanosky (2016), p. 130.
[238] See Biener et al. (2015b), p. 147.

increased deductibles lead to a significant premium reduction, as the moral hazard problem is tackled.[239] Second, the additional services of insurance can help the company. The firm gets access to experts and therefore, gets both preventive support and support in case of damage. If a company decides against insurance, it became clear that it is associated with an organizational extra effort and the other measures such as employee training and crisis planning must not be neglected. Eventually, the overall level of cyber security can be increased due to a appropriate insurance.

8.4 Periodic risk process

Finally, a company will bear part of the risk itself. In actuarial view, the liability is limited by the insurance sum and the defined insurance benefits. Thus, the company bears the deductible and uninsured cases.

Hence, like for every potential damage, companies prepare for an incident by forming an equity reserve. For an independent strategy, capital reserves are not a suitable instrument because the costs due to a cyber attack can shut down the company.

In particular, the previous work identifies two issues a company needs to address in terms of cyber risks. As a result of digitization, they will increasingly come into contact with cyber risks. This happens directly through the use of new technologies or indirectly through affiliated entrepreneurs. Furthermore, insurance companies will also adapt steadily.

Based on this, it is important to understand the management of cyber risks not as a one-off action but to implement a periodic process that manages the problem with the necessary knowledge. As a part of cyber risk management, it became clear that the factors influencing the risk as well as the technical, organizational and insurance aspects are constantly evolving. The biggest mistake a company can make is, therefore, to consider cyber risk as a static problem that needs to be resolved once. As companies periodically deal with the problem, taking out insurance also leads to a sustained higher level of IT security.

[239] See Gordon et al. (2003), p. 83.

9. Summary and Outlook

One of the key findings of this work is that cyber risks have to be taken into account in every company. Digitization affects every business and will continue to change the working environment in the future. In addition to the visible opportunities, the invisible hazards are growing. The master's thesis clarified that the risks of cyber attacks are too great to be neglected in the overall context of risk management. Digitization requires rethinking. This applies not only to business models and processes but also to the risks associated with digital transformation. It is important to be aware of the involved risks, to fill the gaps in risk management. Even if technology-based solutions are the basis of a suitable cyber security precaution, the problem is too complex to tackle one-sidedly. Especially, these investments have to make economic sense in the interests of all stakeholders. In addition, it has became evident that a lot of the dangers originate from the users and their decision. Therefore, state-of-the-art security systems can create a deceptive sense of security without completing the full risk management process.[240]

Appropriate cyber insurance transfers a large part of the residual risk of the company and extends this financial coverage through preventive services that address the main problem: The human factor.

Indeed, cyber insurance does not replace the overall concept of cyber security. Technology, regular updates, periodic employee awareness training, security control, and organized crisis management are measures to counter cyber risks. The effort of a corresponding hedge is great, but also the threats. Cyber insurances have adapted to the circumstances and can be a useful addition to any business. Both SME and large corporations benefit from financial liability and organizational support. As means of attack, technologies and cyber insurance continue to evolve, a periodic review of the overall concept is necessary. Risk managers have to encounter a steady changing problem with a dynamic solution. For this, the minimum term of the insurance for one year is suitable. The field of research dealt with in this work is therefore of great importance in the future as well. In particular, the influence of new technologies such as artificial intelligence may be the subject of further

[240] See Abawajy (2014), p. 238.

research. It will also be interesting to see how the disclosure of cyber attacks is changing as a result of the GDPR.

Thus, in the overall context of risk management, digital risks can be sustainably managed. Such digital risk management is one of the pillars which a successful digitization strategy is ultimately based on. Cyber insurance complete cyber risk management to an overall concept of prevention, damage control, and financial security.

Appendix

Appendix 1: Taxonomy of Cyber Risks[241]

Taxonomy	Decription	Elements
Category 1: Actions of People		
1.1 Inadvertent	Unintended action without malicious intent	mistakes, errors, omissions
1.2 Deliberate	Intended action with malicious intend	fraud, sabotage, theft, vandalism
1.3 Inaction	Lack of action, failure to act	lack of skills, knowledge, guidance or availability of a person
Category 2: Systems and Technology Failures		
2.1 Hardware	Failures in physical equipment	Failure due to capacity, performance, maintenance, obsolescence
2.2 Software	Risks resulting from software assets	Compatibility, configuration management, change control, security settings, coding practices, testing
2.3 Systems	Failures of integrated systems	Design, specifications, integration, complexity

[241] Source: Own representation based on Cebula and Young (2010), pp. 3-8

Category 3: Failed Internal Processes		
3.1 Process design and/or execution	Failure of processes	Process flow, process documentation, roles and responsibilities, notifications and alerts, information flow, escalations of issues, service level agreements, task hand-off
3.2 Process controls	Inadequate controls on the operation of the process	Status monitoring, metrics, periodic review and process ownership
3.3 Supporting processes	Failure of organizational supporting processes to deliver the appropriate resources	Staffing, accounting, training and development, procurement
Category 4: External Events		
4.1 Hazards	Catastrophes, Risks resulting from natural and human events which the organizations have no control	Weather event, fire, flood, earthquake, unrest, pandemic
4.2 Legal issues	Risks arising from legal issues	Regulatory compliance, legislation, litigation
4.3 Business issues	Operational risks arising from business issues	Supplier failure, market conditions, economic conditions
4.4 Service dependencies	Risk arising from the organization's dependence on external parties	Utilities, emergency services, fuel, transportation

Appendix 2: A comparison of selected insurance tariffs[242]

Insurance Company	AXA	Gothaer	HDI	Hiscox	Markel
Tariff	ByteProtect	RAVE-W112010	Cyber-Versicherung	CyberClear up to 1 Mio. € revenue	Markel Pro Cyber incl. all options
Prevention					
Crisis Plan	Yes, Pattern template	Yes, Chargeable depending on the effort	Optional, Chargeable	Yes	Yes
Cyber awareness training	Yes, 6 Month	Yes	Yes, Partner: Perseus	Yes	Yes
Emergency aid on suspicion	Yes (T-Systems Hotline)	Yes (48 h)	Yes (48 h)	Yes (24 h)	Yes
Assistance					
crisis consultant	Yes, Partner: T-Systems	Yes, Partner: infraforce & instinctif	Yes, Partner: Consult	Yes. Partner: HiSolution	Yes, Partner: msg systems AG
Availability	24 h / 7 days	24 h / 7 days	24 h / 7 days	24 h / 7 days	24 h / 7 days
Risk assessment	opt.	opt.	opt.	opt.	opt.
Insured Incidents					
Hacker - Attacks (targeted and untargeted)	Yes	Yes	Yes	Yes	Yes
DoS - Denial of Service	Yes	Yes	Yes	Yes	Yes
Malware (viruses, worms, Trojans)	Yes	Yes	Yes	Yes	Yes
Intentional employee	Yes	Yes	Yes	Yes	Yes
Data infringement	Yes	Yes	Yes	Yes	Yes
operator errors	Yes	Yes	Yes	Yes	Yes
Infringement by advertising & media	Yes	Yes	Yes	Yes	Yes
Limitation					
assistance services	up to the sum insured	up to the sum insured	up to the sum insured	up to the sum insured	up to the sum insured
forensic costs	up to the sum insured	up to the sum insured	up to the sum insured	up to the sum insured	up to the sum insured
business interruption	up to the sum insured	up to the sum insured	up to the sum insured	up to the sum insured	up to the sum insured
Additional costs due to business interruption	up to the sum insured	up to the sum insured	up to the sum insured	up to the sum insured	up to the sum insured
Contractual penalties for breach of confidentiality obligations	up to 25 % of the sum insured (max. 250.000 €)	No	up to 20 % the sum insured	250.000 €	250.000 €
Fines (abroad)	No	Sublimit depends of the sum insured up to max. 250.000 €	up to 20 % the sum insured	250.000 €	up to the sum insured
deductible	1.000 €, 2.500 € or 5.000 €	500 €, 1.000 €, 2.500 €, 5.000 €	1.000 €, 2.500 € or 5.000 € and larger	1.000 €, 2.500 € or 5.000 €	1.000 €, 2.500 € or 5.000 € and larger
Waiver of exclusions					
Intention	Yes, except representative	Yes, except representative	Yes, except representative	Yes, except representative	Yes, except representative
Failure infrastructure	Yes, if telecommunication	No	No	No	No
unlawful data collection	Yes	No	No	No	No
Insolvency	No	Yes	Yes	Yes	Yes
Waiver of subsequent obligations					
Technical	Yes	Yes	Yes	Yes	Yes
testing clause	Yes	Yes	Yes	Yes	Yes
Backup	No 1x/week	No 1x/week	No 1x/week	Yes	Yes
Physical access controls	Yes	Yes	Yes	Yes	Yes
Firewall and Antivirus	No	No	No	Yes	Yes
Insurable industries					
Services	Yes, no financial services	Yes, no financial services	Yes	Yes, no financial services	Yes, no financial services
public companies	Yes	Yes	No	Yes	Yes
Production Business	Yes	Yes	Yes	optional	No
Trade	Yes	Yes	Yes	Yes	Yes
Online-Trade	Yes	Yes	Yes	Yes	Yes
Craft	Yes	Yes	Yes	Yes	Yes

[242] Source: Own representation based on AXA (2018), Hiscox (2019b), Markel (2019), HDI (2019) and Gothaer (2019)

Bibliography

Abawajy, J. (2014): User preference of cyber security awareness delivery method, in: Behaviour & Information Technology, Vol. 33, No. 3, pp. 237-248.

Abbasi, A., R. H. L. Chiang and S. Sarker (2016): Big Data Research in Information Systems: Toward an Inclusive Research Agenda, in: Journal of the Association for Information Systems, Vol. 17, No. 2, pp. 1-32.

AIG (2019): CyberEdge, last accessed on 25.08.2019 at https://www.aig.de/geschaftskunden/produkt-kategorien/financial-lines/cyberedge

Albrecht, P. (2003): Zur Messung von Finanzrisiken, Mannheimer Manuskripte zu Risikotheorie, Portfolio Management und Versicherungswirtschaft, Nr. 143.

Albrecht, J. P. (2016): How the GDPR Will Change the World, in: European Data Protection Law Review, Vol. 2, No. 3, pp. 287-289.

Allianz (2018): AllSecur Kfz-Versicherung PKRB 253/05, last accessed on 25.08.2019 at https://www.allsecur.de/dam/jcr:3ba048ad-5e66-4e8f-934c-239b2f6367cb/versicherungsbedingungen-kfz-KRB253_08premium.pdf

AXA (2018): ByteProtect, last accessed on 25.08.2019 at https://www.axa.de/site/axa-de/get/documents/axade/AXA.de_Dokumente_und_Bilder/Geschaeftskunden/Absicherung-von-IT-und-Cyberrisiken/Risiko-Check-IT-fuer-IT-Anwender.pdf

Bandyopadhyay, T., Mookerjee, V. S. and Rao. R. C. (2009): Why IT Managers Don't Go for Cyber-Insurance Products, in: Communications of the ACM, Vol. 52, No. 11, pp. 68-73.

Bank for International Settlements (2001): Working Paper on the Regulatory Treatment of Operational Risk. Basel Committee on Banking Supervision.

Bank for International Settlements (2006): International Convergence of Capital Measurement and Capital Standards: A Revised Framework. Basel Committee on Banking Supervision

Basel Committee on Banking Supervision (1999): A New Capital Adequacy Framework. Consultative Paper. Bank for International Settlements.

Bayer, U., A. Moser, C. Kruegel and E. Kirda (2006): Dynamic analysis of malicious code, in: Journal in Computer Virology, Vol. 2, No. 1, pp. 67-77.

Bedner, M. and T. Ackermann (2010): Schutzziele der IT-Sicherheit, in: Datenschutz und Datensicherheit, Vol. 34, No. 5, pp. 323-328.

Biener, C., M. Eling, A. Matt and J. H. Wirfs (2015a): Cyber Risk: Risikomanagement und Versicherbarkeit, Verlag Institut für Versicherungswirtschaft der Universität St. Gallen, I·VW Schriftenreihe; Band 54, St. Gallen.

Biener, C., M. Eling and J. H. Wirfs (2015b): Insurability of Cyber Risk: An Empirical Analysis, in: The Geneva Papers on Risk and Insurance - Issues and Practice, Vol. 40, No. 1, pp. 131-158.

Bitkom (2018a): Cloud Computing, Press release from 12.06.2018, last accessed on 23.08.2019 at https://www.bitkom.org/Presse/Presseinformation/Zwei-von-drei-Unternehmen-nutzen-Cloud-Computing.html

Bitkom (2018b): Live Security Studie 2017/2018, last accessed on 23.08.2019 at http://images.secure.f-secure.com/Web/FSecure/%7bd96742c3-f1f1-409c-b179-e78de920f80d%7d_F-Secure_Live_Security_Studie_2017_2018.pdf

Böhme, R., G. Schwartz (2010): Modeling Cyber-Insurance: Towards A Unifying Framework, Working Paper, ICSI and UC Berkeley.

Bouchaud, J.-P., and M. Potters (2000): Theory of Financial Risks. From Statistical Physics to Risk Management. Press Syndicate of the University of Cambridge.

Cebula, J. J. and L. R. Young (2010): A Taxonomy of Operational Cyber Security Risks, Technical Note CMU/ SEI-2010-TN-028, Software Engineering Institute, Carnegie Mellon University.

Choi, I., D. E. Cantor and J. Geroge (2017): Does IT Capability and Competitive Actions Shape Firm Profitability?, in: ICIS 2017 Proceedings 5.

Christoffersen, P. F. (2012): Elements of Financial Risk Management, Academic Press, Elsevier, 2nd. Edition, Oxford.

Cornalba, C. and P. Giudici (2004): Statistical models for operational risk management, in: Physica A: Statistical Mechanics and its Applications, Vol. 338, No. 1-2, pp. 166-172.

DerTreasurer (2017): Leoni Attack, report published at 06.04.2017, last accessed on 27.08.2019 at https://www.dertreasurer.de/news/risiko-management/leoni-arbeitet-fake-president-fall-auf-57521/

Douligeris, C. and A. Mitrokotsa (2004): DDoS attacks and defense mechanisms: classification and state-of-the-art, in: Computer Networks, Vol. 44, No. 5, pp. 643-666.

Eccles, G. E., S. C. Newquist and R. Schatz (2007): Reputation and Its Risks, in: Harvard Business Review.

Eling, M. and W. Schnell (2016): What do we know about cyber risk and cyber insurance?, in: The Journal of Risk Finance, Vol. 17, No. 5, pp. 474-491.

Fayyad, U., G. Piatetsky-Shapiro, and P. Smyth (1996): The KDD process for extracting useful knowledge from volumes of data, in: Communications of the ACM, Vol. 39, Nr. 11, pp. 27-34.

Federal Office for Information Security (2019a): Alliance for cyber security, last accessed on 11.07.2019 at https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Ueber_uns/ueber_uns.html

Federal Office for Information Security (2019b): Cyber-Security-Survey, Press release from 18.04.2019, last accessed on 11.07.2019 at https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Informationspool/Cyber-Sicherheits-Umfrage/CyberSicherheitsUmfrage_2018/umfrage_2018.html?nn=12243794&cms_pos=7

Franke and Bornberg (2018a): Cyber-Rating, Press release from 19.10.2018, last accessed on 22.07.2019 at https://www.franke-bornberg.de/sites/franke-bornberg/files/pressemitteilungen/2018-10-19_Franke_und_Bornberg_PM_Cyber.pdf

Franke and Bornberg (2018b): Valuation Guidelines, last accessed on 22.07.2019 at https://www.franke-bornberg.de/sites/franke-bornberg/files/rating-bewertungsrichtlinien/2018-10-18-Bewertungsrichtlinie-Cyber.pdf

Franke and Bornberg (2019): Cyber-Rating, last accessed on 22.07.2019 at https://www.franke-bornberg.de/ratings/gewerbeversicherung/cyber-versicherung/cyberversicherung

Furnell, S. M. and M. J. Warren (1999): Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium?, in: Computers & Security, Vol. 18, Nr. 1, pp. 28-34.

Gabler Wirtschaftslexikon (2018): Definition of Risk, Release from 19.02.2018, last accessed on 13.07.2019 at https://wirtschaftslexikon.gabler.de/definition/risiko-44896/version-268200

Gabler Wirtschaftslexikon (2019): Definition of Cyber Risk and Cyber Space, Release from 19.02.2018, last accessed on 18.08.2019 at https://wirtschaftslexikon.gabler.de/definition/cyber-risiken-54413/version-277447

Gandotra, E., D. Bansal and S. Sofat (2014): Malware Analysis and Classification: A Survey, in: Journal of Information Security, Vol. 5, pp. 56-64.

GDV (2019): Wer versichert was? , last accessed on 18.08.2019 at https://www.gdv.de/service/wer-versichert-was/de/47406?productQuery=Cyberversicherung&channelId=82

Gordon, L. A. and M. P. Loeb (2002): The economics of information security investment, in: ACM Transactions on Information and System Security, Vol. 5, No. 4, pp. 438-457.

Gordon, L. A., M. P. Loeb and T. Sohail (2003): A Framework for Using Insurance for Cyber-Risk Management, in: Communications of the ACM, Vol. 46, No. 3, pp. 81-85.

Gordon, L. A., M. P. Loeb, W. Lucyshyn and R. Richardson (2005): CSI/FBI Computer Crime and Security Survey.

Gothaer (2019): Gothaer KMU Studie 2019, last accessed on 25.08.2019 at https://gothaer-maklerblog.de/gothaer-kmu-studie-2019-furcht-vor-cyber-attacken/

Haimes, Y. Y. (1991): Total Risk Management, in: Risk Analysis, Vol. 11, No. 2, pp. 169-171.

Hallikas, J., I. Karvonen, U. Pulkkinen, V.-M. Virolainen and M. Tuominen (2004): Risk Management process in supplier networks, in: International Journal of Production Economics, Vol. 90, No. 1, pp. 47-58.

HDI (2019): Cyber, last accessed on 25.08.2019 at https://www.hdi.global/de/de/versicherungen/haftpflicht-financial-lines/cyberversicherung

Hiscox (2019a): Hiscox Cyber Readiness Report 2019, last accessed on 18.07.2019 at https://www.hiscox.de/wp-content/uploads/2019/04/Hiscox-Cyber-Readiness-Report-2019.pdf

Hiscox (2019b): Hiscox CyberClear Bedingungen 03/2019, last accessed on 25.08.2019 at https://makler.hiscox.de/sites/default/files/2019-03/bedingungen-hiscox-cyberclear-daten-versicherung-032019.pdf

IBM (2019): X-Force Threat Intelligence Index, last accessed on 22.08.2019 at https://www.ibm.com/security/data-breach/threat-intelligence

International Data Corporation (2018): Data Age 2025, The Digitization of the World, From Edge to Core, IDC White Paper, last accessed on 15.08.2019 at https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf

International Data Corporation (2019): The Growth in Connected IoT Devices, Press release from 18.06.2019, last accessed on 15.08.2019 at https://www.idc.com/getdoc.jsp?containerId=prUS45213219

International Organization for Standardization (2018): ISO 31000:2018 Risk management - Guidelines, last accessed on 20.08.2019 at https://www.iso.org/obp/ui/#iso:std:65694:en

International Telecommunication Union (2008): Overview of cybersecurity, Series X: Data Networks, Open System Communications and Security, ITU-T X.1205.

Jouini, M., L. Ben Arfa Rabai and A. Ben Aissa (2014): Classification of security threats in information systems, in: Procedia Computer Science, Vol. 32, pp. 489-496.

Kaplan, S. and B. J. Garrick (1981): On the Quantitative Definition of Risk, in: Risk Analysis, Vol. 1, No. 1, pp. 11-27.

Kloman, H. F. (1990): Risk Management Agonistes, in: Risk Analysis, Vol. 10, No. 2, pp. 201-205.

KPMG (2017): Digitalisierung und Cyber Studie 2017, last accessed on 26.08.2019 at https://assets.kpmg/content/dam/kpmg/ch/pdf/neues-denken-neues-handeln-cyber-de.pdf

KPMG (2019): e-crime in der deutschen Wirtschaft, last accessed on 26.08.2019 at https://hub.kpmg.de/studie-e-crime-in-der-deutschen-wirtschaft-2019

Kulikova, O., R. Heil, J. van den Berg, J. and W. Pieters (2012): Cyber Crisis Management: A decision-support framework for disclosing security incident information, in: International Conference on Cyber Security 2012, pp. 103-112.

Lai, C., G. Medvinsky und B. Clifford Neuman (1994): Endorsements, licensing, and insurance for distributed system services, in: Proceedings of the 2nd ACM Conference on Computer and communications security, pp. 170-175.

Loch, K. D., H. C. Carr and M. E. Warkentin (1992): Threats to Information Systems: Today's Reality, Yesterday's Understanding, in: MIS Quarterly, Vol. 16, No. 2, pp. 173-186.

Markel (2019): Markel PRO Cyber, last accessed on 25.08.2019 at https://markel.de/maklerportal/markel-pro-cyber

Marotta, A., F. Martinelli, S. Nanni, A. Orlando and A. Yautsiukhin (2017): Cyber-Insurance Survey, in: Computer Science Review, Vol. 24, pp. 35-61.

McAfee, A. and E. Brynjolfsson (2012): Big Data: The Management Revolution, in: Harvard Business Review, Vol. 90, No. 10, pp. 1-9.

McNeil, A. J., R. Frey and P. Embrechts (2015): Quantitative Risk Management: Concepts, Techniques and Tools, Princeton University Press, Revised Edition.

Mukhopadhyay, A., S. Chatterjee, D. Saha, A. Mahanti and S. K. Sadhukhan (2013): Cyber-risk decision models: To insure IT or not?, in: Decision Support Systems, Vol. 56, pp. 11-26.

Palmrose, Z.-V., V. J. Richardson and S. Scholz (2004): Determinants of market reactions to restatement announcement, in: Journal of Accounting and Economics, Vol. 37, No. 1, pp. 59-89.

Perry, J. and P. de Fontnouvelle (2005): Measuring Reputational Risk: The Market Reaction to Operational Loss Announcements, Federal Reserve Bank of Boston, last accessed on 20.08.2019 at https://ssrn.com/abstract=861364

Pohlmann, N. (2006): Wie wirtschaftlich sind IT-Sicherheitsmaßnahmen?, Institut für Internet-Sicherheit, HMD-Praxis Wirtschaftsinformatik

Ponemon Institute (2010): 2010 Annual Study: Global Cost of a Data Breach, last accessed on 20.08.2019 at https://www.symantec.com/content/dam/symantec/docs/reports/cost-of-data-breach-global-report-2010-en.pdf

Provinzial (2019): Cyber Versicherung, last accessed on 19.08.2019 at https://www.provinzial-online.de/content/firmen/versicherungen/haftung-und-recht/cyberversicherung/

Romanosky, S. (2016): Examining the costs and causes of cyber incidents, in: Journal of Cybersecurity, Vol. 2, No. 2, pp. 121-135.

Seibold, H. (2006): IT-Risikomanagement, München.

Sharma, R., S. Mithas and A. Kankanhalli (2014): Transforming decision-making processes: a research agenda for understanding the impact of business analytics on organisations, in: Risk, Vol. 23, No. 4, pp. 433-441.

Siegel, C. A., T. R. Sagalow and P. Serritella (2002): Cyber-Risk Management: Technical and Insurance Controls for Enterprise-Level Security, in: Information Systems Security, Vol. 11, No. 4, pp. 33-49.

Smith, C. W. and R. M. Stulz (1985): Determinants of Firms' Hedging Policies, in: The Journal of Financial and Quantitative Analysis, Vol. 20, No. 4, pp. 391-405.

Smithson, C. and P. Song (2000): Quantifying Operational Risk, in: Risk, Vol. 17, pp. 57-59.

Sonnenreich, W., J. Albanese and B. Stout (2006): Return on Security Investment (ROSI) – A Practical Quantitative Model, in: Journal of Research and Practice in Information Technology, Vol. 38, No. 1, pp. 45-56.

Statista (2019): Cyber Attacks, last accessed on 24.08.2019 at https://de.statista.com/statistik/daten/studie/1013758/umfrage/umfrage-zu-den-gruenden-erfolgreicher-cyber-attacken-in-deutschland/

The Register (2010): Google Attack, report published at 14.01.2010, last accessed on 27.08.2019 at https://www.theregister.co.uk/2010/01/14/google_china_attack_analysis/

Trautman, L. J., J. Triche and J. C. Wetherbe (2013): Corporate Information Technology, Governance under Fire, in: Journal of Strategic and Internal Studies, Vol. 8, No. 3, pp. 105-114.

Valentine, J. A. (2006): Enhancing the employee security awareness model, in: Computer Fraud & Security, No. 6, pp. 17-19.

Wood, C. C. (2004): Why information security is now multi-disciplinary, multi-departmental, and multi-organizational in nature, in: Computer Fraud & Security, No. 1, pp. 16-17.

World Economic Forum (2019a): The Global Risks Report 2019, last accessed on 20.08.2019 at https://www.weforum.org/reports/the-global-risks-report-2019

World Economic Forum (2019b): Global Risks Report 2019 , Press release from 16.01.2019, last accessed on 20.08.2019 at http://reports.weforum.org/global-risks-2019/press-release/

Zerlang, J. (2017): GDPR: a milestone in convergence for cyber-security and compliance, in: Network Security, No. 6, pp. 8-11.

Declaration of Authorship

Declaration[243]

I,

Surname, First name: Bechtle, Christoph Rudolf
Matriculation number: 618383

declare that I have followed the Principles of Good Scientific Practice while writing the present
☐ Master's thesis

I have written the paper/thesis independently and have used no other sources or aids than those given and have marked the passages taken from other works word-for-word or paraphrased.

Supervisor: Prof. Dr. Jörg Schiller

Topic of the thesis:
Cyber-Risk Management – a framework for companies to react to a constantly changing risk including a supply comparison of the German insurance market

Semester: Summer term 2019

I furthermore declare that the submitted unencrypted electronic document exactly and without exception corresponds to the contents and wording of the printed copy of the paper/thesis. I give my consent to this electronic version being checked for plagiarism with analytical software.

Stuttgart, 04.09.2019, _____

[243] This declaration is to be included into the independently written paper/thesis as an annex. Papers/theses not including this declaration will not be accepted.