WILHELM

RECHTSANWÄLTE

Christian Drave, LL.M. Versicherungspraxis June 2015

Emerging Risks

Cyber risks: a challenge for risk management

1. INTRODUCTION

Cyber risks, as so-called „emerging risks“, pose particular challenges to risk management and the insurance purchasing of companies. These challenges equally concern risk-assessment, - avoidance and – transfer. Possibilities and problems concerning the handling of cyber risks and their insurance are presented in the following.

2. DAMAGE POTENTIALS AND RISK ANALYSIS

The term cyber risk is not clearly defined. Part of a company’s risk management is though the handling of all relevant risks, independent of the kind and qualification of risks.

In a first step, risk management requires that the policy holder identifies the risks existing within the company. Subsequently, the damage potential has to be determined. How probable is the occurrence and what’s the possible amount of the damage? This assessment has particularities for cyber risks and -damages.

2.1 Potentials for own damages and liability damages

Cyber risks mainly cause financial losses. Here, two kinds of damages have to be identified: own damages and liability damages, thus third-party losses. The policy holder’s own damages caused by cyber risks are for example the loss of intellectual property, e.g. by targeted theft of product and development information.

Damages resulting from business interruptions have severe practical relevance. They may easily reach a scope endangering the company's existence – independent of whether for example a steel factory's operation is interrupted or an online retailer is not able to perform his distribution after a hacker attack.

Damages might also affect the property of third parties (third party damages/liability damages). Those might be contract partners of the own company, such as for example the consumer or the respective partner within the supply chain with whom data is exchanged. Stronger outsourcing tendencies increase the number of contract partners.

From risk management's point of view different questions arise: Is an analysis and optimization of the own IT security sufficient? Or does the company have to provide, e.g. by respective design of contract, for external service providers to work with equal standards? What are the risks to cause damage to third parties and thus cause a liability claim?

2.2 Risk analysis

The risk analysis has to consider that the legal situation in the area of IT security has changed both nationally and internationally. The risks for companies and the requirements on security structures are changing accordingly.

The German Federal Government for example intends to tighten the requirements to companies concerning data security with a current draft of the new IT security act. The draft provides for comprehensive information, documentation and reporting obligations and a cooperation with the relevant authority (Federal Office for Information Security, BSI).

The same applies in an international context. In the USA, the so-called cyber security act shall affect a cooperation between US companies and the government in the fight against cyber perils. This law initiative is especially interesting with regard to imminent third party liability claims. The intent of the law is to protect companies that cooperate with authorities and exchange information about cyber risks from claims of third parties such as customers or shareholders.

The risk analysis has to be related to the company. Companies that use numerous customer data such as credit card information have a severe risk to lose person related data. The company is obliged to inform the authority and all persons affected about the

loss of data (cp. sec. 42 a Federal Data Protection Act "BDSG"). In this case, millions of data may cause severe damage. It's though different for the producing industry. Here, the focus is possibly on an interruption of the IT-steered production line.

The determined risks are to be evaluated according to their occurrence probability and the amount of the damage. Here, immense importance will be on the question of economic impacts of damage scenarios.

2.3 Risk analysis through the insurer?

From the policy holder's point of view it makes sense to include external specialists into the risk analysis, since stress tests of the IT (e.g simulated hacker attacks) should be performed from outside the system and not by persons familiar with the system.

In the context of selling cyber policies, insurers offer to make a risk analysis at the policy holder's site. The insurers usually cooperate with specialized IT service providers. From the policy holder's point of view it should be considered that often the same service provider will establish the proof of damage after occurrence of the insured event and won't preferentially focus on the policy holder's interests. It is thus advisable to consult (eventually additional) own external experts.

3. RISK REDUCTION OR RISK TRANSFER?

After the risk analysis it has to be checked in how far and at what costs risks may be avoided resp. reduced or transferred to other risk carriers resp. be retained by the company itself.

In this context it is decisive that cyber risks are mainly technical and organizational risks. The reduction mainly requires investments in IT infrastructure and company organization (e.g. by means of clear procedures and data protection regulations for employees as well as a consequent realization and control). This requires an interdisciplinary risk management in cooperation with all relevant competences (e.g. risk management, IT, insurance, compliance, controlling and data protection). Depending on the kind of risk it has to be assessed which handling of individual risks (e.g. upgrading the IT infrastructure, restructuring of internal processes, insurance) are economically reasonable and technically expedient.

4. RISK TRANSFER BY INSURANCE

For risks which the policy holder does not want to reduce or is not able or willing to bear, the question of a risk transfer by the insurance arises.

4.1 Analysis of existing insurance cover

In the individual case, cyber risks might be covered by existing insurance contracts. A respective analysis has to be performed under consideration of the company's own risks and the individually existing insurance program.

4.2 Addition to existing policies vs. purchase of a cyber policy

The policy holder may include cyber risks into already existing policies or purchase separate cyber insurances.

Whether an extension of cover or a separate cover is reasonable depends on the kind of risk and the policies already existing in the individual case. If the company's risk focus lies for example on business interruptions, the company will have a business interruption insurance. Here it might be expedient to negotiate with the insurer in order to include cyber risks into the insurance cover - since from the policy holder's point of view it is irrelevant whether the business interruption results from fire or a hacker attack (loss of production related data). This will though be different e.g. for companies working in the health sector who deal with a high number of sensible information (loss of person related data).

4.3 Aspects of cover

Cyber insurances available on the market severely differ with regard to their scope of cover.

4.3.1 Inconsistent cover standards

For policy holders it's a challenge that the cyber insurance market currently has no consistent standard of cover. Cyber covers usually distinguish among own damages and liability damages (third party losses) as well as other elements of cover. There are though no consistent regulations about the insured event, exclusions and obligations as well as the consequences of breaches of obligations. While for example many insurance terms follow the quo rata principle of the Insurance Contract Act (VVG), others follow the "All-

or-nothing-principle" and thus the insurer's entire release from payment as a sanction for gross negligent breaches of obligations.

4.3.2 Differentiation of insurance contracts

In order to avoid cover gaps and double insurance, policy holders have to differentiate cyber insurance policies from existing insurance contracts. Here it is especially important to put a focus on clear definitions of the insured event and exclusions to make clear when cover is granted. In cyber policies, exclusions shall be avoided which correspond with exclusions of existing industrial insurance contracts.

Besides, subsidiarity clauses of cyber policies and the existing contracts have to be reviewed and evaluated according to relevant jurisdiction in order to determine which insurance cover might exist subordinately.

4.3.3 Additional services

Cyber policies offer additional services. The insurer might in the insured event for example provide the policy holder with IT-forensics to recover the system and restore data or to provide experts such as PR experts for crisis management or lawyers to defend against claims. Such parts of service regularly make up a large portion of the premium. From the policy holder's point of view the necessity of additional services has to be examined carefully against the background of already existing resources and service providers.

4.3.4 Uninsurable risks

What has to be considered when purchasing insurance cover is that major damage potential in connection with cyber risks are (currently) uninsurable.

4.3.4.1 Reputation damages and loss of intellectual property

Cyber damages might cause severe reputational damages. Such damages are difficult to estimate and are therefore uninsurable. The same applies for the loss of intellectual property.

4.3.4.2 Fines?

Relevant cyber risks include the risk that the insured company has to pay fines resulting from severe breaches against data protection regulations. Such fines might amount to up to EUR 300,000.00 according to the Federal Data Protection Act (BDSG), in case of a possible skimming of excess profits even higher. The importance of this risk might even increase. The intended EU data protection regulation aims at fines which are many times higher.

Cyber cover regularly excludes fines from insurance cover. The insurance industry argues that fines are uninsurable for legal reasons. According to the view represented here, this does not generally apply. The question of insurability of fines is thus legally not clear yet – among others also against the background of current civil and labor law procedures about the reimbursement of fines. The question of insurance cover for fines should also be further discussed from the policy holder's point of view, especially since fines imply a severe damage potential.

4.4 Missing claims experience

Cyber insurances are a comparably new product. Policy holders and partly insurers are missing claims experience, especially since the damages can be very different. Thus it is even more crucial to have clear provisions about the settlement of damages in the insurance contract.

5. CONCLUSION

Cyber risks pose common challenges to the policy holding industry and the insurance industry. From the policy holder's point of view, the handling of cyber risks is part of an adequate risk management which implies a thorough identification of risks and the development of damage prevention strategies.

The insurance of cyber risks especially implies the danger of cover gaps or multiple insurance. Inconsistent cover concepts make it difficult for the policy holder to gain an overview of the still young market for cyber insurances. A regular analysis of the own risks and their insurability through new insurance solutions is therefore an important task of cyber risk management.

Christian Drave, LL.M.
Lawyer
Master of Insurance Law

Wilhelm Partnerschaft von Rechtsanwälten mbB
Reichsstraße 43
40217 Düsseldorf

Tel: +49 211 687746 43
Fax: +49 211 687746 20

www.wilhelm-rae.de
christian.drave@wilhelm-rae.de