WILHELM

RECHTSANWÄLTE

Christian Drave, LL.M. Versicherungspraxis, April 2016

Cyber Insurance

Cyber risks and insurance: current status and developments

Surveys and analyses confirm that cyber risks are perceived as "top risks" by many companies. Exposed cyber incidents in the recent past have contributed to this view. Tighter requirements to data security, own losses potentially threatening the existence and a shift of liability impose challenges on risk managers and insurers.

Do you worry about cyber risks? My colleague most certainly does, and even physically. This is not only the case because he is responsible for IT. My colleague rather experienced himself the impacts of threats from the cyber space. Only recently he had to go to hospital in the Rhine area during the night with acute abdominal pain. You may already suspect: This hospital was one of those that became a victim of targeted cyber-attacks through encryption Trojans (ransomware). As a consequence, doctors were not able to provide acute treatment (though according to information by the hospitals affected, the medical treatment of patients has not been endangered at any time). My colleague was transported to another hospital. Luckily he is well again – in contrast to the IT-infrastructure of the affected hospital, as reported by media.

The German Federal Office for Information Security ("BSI") refers in connection with cyber-attacks to hospitals in a press release of 8th March 2016 to the current threat situation for critical infrastructures, thus companies and institutions providing social services:

„Due to their exceptional importance for the well-being of the population, hospitals are an important part of critical infrastructures. Therefore, they have a particular obligation to secure the availability of their services…"

Not only against the background of cyber-attacks to hospitals, the German Bundestag or Sony the questions about the status and tendencies concerning cyber risks and their insurance arise. This article examines the concrete danger and the risk awareness in connection with cyber risks and shows on the basis of selected individual subjects developments which equally challenge policy holders and insurers.

Potential danger and risk awareness

Experts observe that attacks to the information infrastructure in the cyber field on the one hand become more and more complex und professional. On the other hand, the companies', state's and population's dependency on IT and thus the damage potential is increasing steadily.[1]

The risk landscape regarding to cyber risks is changing. This applies as well for the legal environment. The IT Securities Act of 2015 obliges the operators of critical infrastructures to grant enhanced security standards for their IT systems. On 15th December 2015, the EU Parliament, the Council of Ministers and the EU Commission agreed on a final version of the EU Basic Regulation on Data Protection, in order to achieve a common European standard for data protection. Since 24th February 2016, especially consumer protection associations have a right to claim in case of data protection breach (reached by the law to enhance the civil law assertion of consumer protecting provisions of the data protection law). Thus, in case of breaches of particular data protection provisions, companies are not only threatened with sanctions of the supervisory authority such as fines, but also with actions for an injunction by consumer protection associations.

The legislative initiatives do not only establish risks for companies in case of breaches, but also illustrate the change in the general risk awareness. This change also has the effect that industry and state institutions increasingly develop standards for IT security. For example, the leading international norm for information security management systems ISO 27001 regulates requirements for the implementation, realization, supervision

[1] Cf. the report on the status of IT-security in Germany 2015 of the German Federal Office for Information Security, retrieved on 10 March 2016 under: https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html;jsessionid=551CE477F3D86D2703E97A41707F2B9D.2_cid294

and improvement of information security management systems. Such standards may have impacts on the definition of obligations to diligence and duties of care (e.g. concerning the question when a conduct is negligent, thus "does not take the reasonable care" or in the field of product liability in the context of the question whether a product corresponds with the latest state of science and technology).

The subject cyber risk has for some time now been called a "management issue" and has arrived as such: requirements to the IT security concern the company's organization and are as such a management task of the responsible managers. The executive board is obliged to prevent risks from companies, which might threaten its existence (cf. sec. 92 para. 2 German Stock Corporation Act "AktG"). The risk prevention also comprises the case that a risk analysis comes to the conclusion that cyber risk might endanger the existence of the company. The (entire) executive board is responsible for company compliance – with the risk of personal liability in case of breaches. Company compliance also includes the area data protection and data security. It is thus the central task of risk management to determine and analyze cyber risks and to take measures to minimize risks or transfer them by means of insurance. In this context companies put a focus on risk minimization through enhancement of their IT security and organization.

Limits to the insurability of own losses

The market of cyber insurances is developing, the same do capacities. Not all cyber risks are though insurable and the obtainable coverage has limits. Due to their economic importance, possible own losses are rightly in the focus of risk assessment.

Own losses may for example hit the company if it loses development data (thus intellectual property) through an external cyber-attack or theft by employees. In particular in case of business interruptions resulting from system breakdowns or – as in the example attacked of hospitals – blocking of data/systems may cause severe damages. Usual cover modules of cyber policies cover own losses caused by business interruptions within certain liability periods and limits.

The risk of penalties imposed by authorities for data protection violations by companies will gain importance. According to indemnity law, penalties are part of the possible own losses of policy holders, even though cyber policies partly classify penalties as liability cases (and thus treat them like third party losses). Concerning the insurance of penalties, the insurers' offers for cover differ strongly.

Reputation risks rightly come more and more into the focus of companies. In particular if it's about the loss of personal customer data, the risk of reputational damages for companies is obvious. But also for company managers, personal risks in connection with cyber threats may exist. For instance, the chairman of the US-retailer Target resigned after a hacker attack, which caused the loss of 40 million credit and payment cards data of customers in 2013. After the spectacular hacker attack against Sony-Pictures at the end of 2014, the co-chief left the company. Cyber policies may compensate part of financial damages of companies via assistance payments such as the assumption of costs for the crisis communications, but will usually only pay within small sublimits. Separate reputational policies may possibly cover damages resulting from drops in sale which are often hardly quantifiable.[2]

Shifting liability risks: Cyber security and product liability

Besides afore described risk of own damages, a wide range of liability risks for companies exists. The progressive digitization and networking in cyber space may lead to a shift of liability risks, in particular in the field of product liability. The following examples from the "digitalized mobility" sector illustrate this development.

Aviation.

It is assumed that the traffic density in international aviation will double within the coming 20 years[3]. Experts agree that the challenges of an increasing traffic density are not manageable with existing management systems. Therefore there are increasingly efforts to standardize and synchronize aviation management (e.g. in the European area by an initiative of the European Commission). The aim is to link all players of aviation such as pilots and air traffic controllers in order to achieve a secure and efficient aviation management.

Networking may also optimize the working conditions of air traffic controllers. Air traffic controllers usually work in shifts. If airports are connected and air traffic control is syn-

[2] Cf. Klinkhammer, Versicherungspraxis 3/2016, p. 3 et seqq.

[3] Cf. article in Schadenspiegel Munich Re 2/2015, p. 6 et seqq., retrieved on 10 März 2016 under: http://www.munichre.com/site/touch-publications/get/documents_E-1212395301/mr/assetpool.shared/Documents/5_Touch/_Publications/08791_SSP_2_2015_de.pdf

chronized, an air traffic controller in Perth may take over the work of his colleagues in another time zone – e.g. in England – and thus avoid night work.

The risk potential of a connected air space in real time is obvious. Data security and data availability are essential and endangered by external attacks. Independent thereof, an increasing digitalization increases product liability risks of systems manufacturers. One of the most serious civil aviation accidents in 2002 was, according to the assessment of the civil court in charge, based on a product defect. The court explained the collision of two airplanes by a construction and instruction defect of the producer of the collision warning system on board. This case shows that a digitalization may on the one hand avoid damages caused by human error and thus reduce the operator's liability risk (through enhanced collision warning systems). On the other hand, the liability risk is shifted from the operator to the systems producer (whose systems have to meet a more and more complex risk situation) [4]. Companies and insurers have to take this shifting of risk into account.

Connected driving and Big Data:

Also the development towards digitalized driving has impacts on product liability risks.

At first, producers have to ensure the (data) security also in the multi-digital system automobile. This aspect gains importance with the increasing digitalization level. Incidents of hackers who took over the control of driving cars, are known and might still happen in the future.

Besides, automobile manufacturers have to collect and process a large amount of data in connection with the operation of their products – and possibly also security-relevant data. Thus, the question about the consequences of this availability of data amounts („Big Data") with regard to a possible product liability of the producer comes up.

If the producer has security-relevant knowledge from its comprehensive data, e.g. about system weaknesses of a car or accident risks, he has to use this information in view of product security. This applies to the product development according to the latest state of science and technology, but also to the observation of own products already

[4] Cf as above, p. 12 with further references.

released for consumption within the framework of producer's obligations. Eventually, a producer is obliged to an earlier warning or product recall, because he has knowledge about possible dangers from its product - eventually transmitted in real time from interconnected vehicles. Big Data faces the producer with the task to provide a company organization which ensures the processing of data from the point of view of product security.[5] An increased digitalization may make driving more secure and in particular minimize damages resulting from human failure. It though transfers responsibilities to the producers. The requirements on security of products increases, and thus finally the risk of product liability.

New approaches and coverage concepts requested

Whether the subject causes worries or not – companies and insurers are right in thinking about cyber risks. Legislative initiatives on data protection and efforts to create common IT security standards may help to cope with cyber risks. Possible liability risks for companies though increase in case of breaches of data protection. Liability risks and the risk of severe own losses set the subjects IT-/data-security and insurance protection in the focus of management.

The progressive digitalization and the related cyber risks also have impacts of "classic" risks and their insurance. This applies in particular to the area product liability. The higher the degree of digitalization of products and processes, the higher will be the possible exposure to risks. Examples from aviation and connected driving show that liability risks shift – from operator, pilots or driver to the producer of the systems, which are supposed to grant secure flying or driving.

Policy holders have to consider the developments described within the context of their risk management. Insurers are facing the challenge to provide appropriate insurance coverage taking these developments into account. This requires new approaches and coverage concepts.

[5] Cf. instructive Hartmann, DAR 2015, 122 et seqq.

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