Management von Cyberrisiken mittels Cyberversicherung

Cyberrisiken gelten aus Unternehmenssicht als eine der „gefährlichsten" Risikoarten. Cybervorfälle führen in etlichen Fällen nicht nur zu Schäden in der eigenen unmittelbaren Unternehmenssphäre, sondern weiten sich auf Dritte aus mit daraus folgenden Haftungsansprüchen. Entsprechend wird dem Management von Cyberrisiken verstärkt Augenmerk zuteil, nicht nur in Großunternehmen, sondern zunehmend auch bei KMU und Kleinstunternehmen. Ein Instrument zur Bewältigung der finanziellen Folgen von Cybervorfällen stellt die Cyberversicherung dar. Ursprünglich mit massiven Wachstumsprognosen versehen, sind zwischenzeitlich Fragen zur Versicherbarkeit von Cyberrisiken und damit zusammenhängende Bewertungsfragen wieder deutlich stärker in den Vordergrund gerückt.

Prof. Dr. Thomas Hartung
ist Professor für Versicherungswirtschaft und Risikomanagement an der Universität der Bundeswehr München. Bevorzugte Forschungsgebiete: Risikomanagement, Versicherungsökonomie, Regulierung, Versicherungsmanagement.

Summary: From a corporate perspective, cyber risks are considered one of the most „dangerous" types of risk. Cyber incidents often not only cause damage within the company's own immediate sphere but can also affect third parties, leading to liability claims against the company. Consequently, the management of cyber risks is receiving increasing attention, not only in large corporations but also progressively among SMEs and micro-enterprises. One instrument for addressing the financial consequences of cyber incidents is cyber insurance. Initially projected to grow significantly, questions about the insurability of cyber risks and related assessment issues have recently regained attention.

Stichwörter: Cyberrisiko, Risikomanagement, Cyberversicherung

1. Bedeutungszuwachs von Cyberrisiken

Cyberrisiken haben sich von einem Nischendasein in den 1990er Jahren, das eher IT-Spezialisten und Akteuren im „Cyberraum" geläufig war, zu einer der gesamtgesellschaftlich **bedrohlichsten Risikokategorien** entwickelt. Das von *Allianz Commercial* jährlich veröffentlichte Risk Barometer, das auf Befragungen von über 3700 Risikomanagern weltweit basiert, führt Cyberrisiken seit 2020 an der Spitze der „Hitliste" der für Unternehmen bedrohlichsten Risiken (vgl. *Allianz Commercial*, 2026). Wie aus aktuellen Veröffentlichungen entnehmbar ist, betreffen Cybervorfälle nicht nur namhafte Großunternehmen und -organisationen, sondern im Grunde Betriebe und Verwaltungen aller Couleur – und zwar täglich (vgl. *DSGVO-Portal*, 2026).

Der Bedeutungszuwachs von Cyberrisiken ist im Einklang mit den Fortschritten der digitalen Transformation zu sehen: Um so vernetzter wirtschaftliche, politisch-administrative und private Akteure werden, desto mehr nimmt das aus dieser Vernetzung resultierende Risikoexposure zu. Entsprechend bedarf es eines planvollen Umgangs damit, speziell durch Integration in die Risikomanagementpraxis (vgl. *Hunziker/Trachsel*, 2023). Neben der Identifikation und der Bewertung von Cyberrisiken sind **risikopolitische Maßnahmen** abzuwägen, mit denen ein zufriedenstellendes Sicherheitsniveau erreicht werden soll. Die Versicherung von aus Cyberrisiken resultierenden Schäden ist eine

Möglichkeit, um zumindest finanzielle Folgen aus solchen Vorfällen einzudämmen.

Eindrücke, welche **Schadendimensionen** mit Cyberrisiken verbunden sein können, werden vor allem aus bisherigen Ereignissen und darauf bezogenen Hochrechnungen gewonnen. So führte beispielsweise ein im Juli 2024 missglücktes Update des Cybersicherheitsdienstleisters *Crowdstrike* für seine Sicherheitssoftware *Falcon* zu globalen Ausfällen bei mit *MS Windows* betriebenen Rechnersystemen – Schätzungen zufolge bei etwa 8,5 Millionen Geräten, darunter auch welche in kritischen Infrastrukturen wie Energieversorgern, Fluggesellschaften oder Krankenhäusern. Der daraus resultierende Gesamtschaden wird auf mindestens 10 Mrd. USD taxiert. Im Nachgang wirft dieser Vorfall die Frage auf, ob bzw. unter welchen Bedingungen die finanziellen Folgen durch Versicherung gedeckt sind sowie welche Schadendimensionen bei umfangreicheren Schadenereignissen vorstellbar wären (vgl. *Drefke*, 2025). Werden beispielsweise die durchschnittlichen Kosten eines erfolgreichen Ransomwareangriffs in Höhe von 5,08 Mio. USD als Grundlage herangezogen (vgl. *IBM*, 2025, S. 5), können Vorstellungen entwickelt werden, welche Folgen weltumspannende Angriffe mit zahlreichen betroffenen Organisationen – wie beispielsweise der *WannaCry*-Ransomware-Angriff 2017 – heutzutage erzeugen können.

2. Cyberrisiko – Begriffseingrenzung und Begriffsinhalte

Der Begriff des Cyberrisikos unterliegt vielfältigen Definitionsansätzen (vgl. beispielsweise *He* et al., 2024, S. 271 f.). Häufig erfolgt aber die Einordnung in die Kategorie der **operationellen Risiken**. Allerdings geht der Begriffsinhalt in den Randbereichen über das hinaus, was vor allem aus regulatorischer Perspektive operationelle Risiken beinhalten – beispielsweise durch die Einbeziehung des Reputationsrisikos (vgl. z.B. *Biener/Eling/Matt/Wirfs*, 2015, S. 7). Eine zu unspezifische Sichtweise führt dazu, dass unter dem Begriff des Cyberrisikos eine Vielzahl unterschiedlicher konkreter Risikoereignisse subsumiert wird, angefangen von singulären Hardwareausfällen bis hin zu weltumspannenden „Computerviruspandemien". Die daraus resultierende Unklarheit über den exakten Begriffsinhalt ist einer der Gründe, die als Hindernis für die fortschreitende Entwicklung eines entsprechenden Versicherungsmarktes angeführt werden (vgl. z.B. *Tsohou* et al., 2023, S. 745). Der Aufgabe, eine disziplinübergreifende und alle wesentlichen Facetten des Cyberrisikos umfassende Definition zu entwickeln, haben sich daher u.a. *Zängerle* und *Schiereck* angenommen (vgl. *Zängerle/Schiereck*, 2023). Ausgangspunkte ihrer Untersuchung sind eine systematische Literaturrecherche und die Analyse von 26 identifizierten Definitionsansätzen. Mithilfe eines Kategoriensystems, das die wesentlichen Merkmale von Cyberrisiken widerspiegelt (vgl. *Zängerle/Schiereck*, 2023, S. 218; *Böhme/Laube/Riek*, 2019, S. 167), entwickeln sie eine **Taxonomie** gemäß *Tab. 1* und den daraus abgeleiteten Vorschlag einer übergreifenden und vereinheitlichten **Definition**: „Cyberrisiken umfassen Bedrohungen aus dem Cyberraum, welche aufgrund einer Schwachstelle sowohl materielle als auch immaterielle Werte als auch Menschen gefährden, was zu direkten und indirekten Schäden einer betroffenen Einheit und von Dritten führen kann." (*Zängerle/Schiereck*, 2023, S. 222; zu anderen Taxonomien siehe *He* et al., 2024, S. 272 f.).

Bedrohungen	Schwachstellen	Risikoobjekte	Auswirkungen
beabsichtigt	*Hardware*	*Materiell*	*direkt*
- Betrug	- Kapazität	- Hardware	- Schäden
- Sabotage	- Leistung	- Software	- Betrieb
- Diebstahl	- Instandhaltung		- Finanzen
- Vandalismus		*Immateriell*	
	Software	- Informationen	*indirekt*
unbeabsichtigt	- Design	- Dienstleistungen	- Sicherheit
- Fehler	- Integrität		- Reputation
- Irrtum	- Komplexität	*Menschen*	- Rechtsbelange
- Versäummis		- physisch	
	Organisation	- psychisch	*Dritte*
	- Prozesse		- direkt
	- Kenntnisse		- indirekt
	- Menschen		

Quelle: *Zängerle/Schiereck*, 2023.

Tab. 1: Taxonomie für Cyberrisiken

Als Vorteil dieser Definition wird ihr disziplinübergreifender Ansatz gesehen. Ihr Abstraktionsgrad wird durch die mitgelieferte Taxonomie gemindert. Zudem können die Überlappungen mit und Abgrenzungen zu ebenfalls in ähnlichem Kontext verwendeten Begriffen wie **Informationstechnologierisiko** (IT-Risiko) oder **Informationssicherheitsrisiko** (IS-Risiko) aufgezeigt werden (vgl. *Zängerle/Schiereck*, 2023, S. 224 f.). Eine einheitliche Terminologie in Sachen Cyberrisiko nützt der **Standardisierung** von Vorgaben im Rahmen von Regulatorik. Aber auch zur Etablierung von Cyberversicherungslösungen ist ein möglichst einheitliches Verständnis aller Beteiligten, welche konkreten Vorfälle abgesichert sein sollen, zweckmäßig.

3. Cyberversicherung

3.1. Marktlage und historische Entwicklung

Die Cyberversicherung gilt per dato als eines der zukunftsträchtigsten, aber auch dynamischsten Versicherungsprodukte. Der **weltweite Cyberversicherungsmarkt** umfasst inzwischen etwa 15 Mrd. US-Dollar an Prämienvolumen, was aber nach wie vor weniger als 1 % der weltweiten Schadenversicherungsprämien entspricht, sodass ein erheblicher und beständiger „**Protection Gap**" – gemessen als Abstand zwischen potenziellen wirtschaftlichen und versicherten Schäden – konstatiert wird (vgl. *Pain*, 2024, S. 9). Gemäß der *Bundesanstalt für Finanzdienstleistungsaufsicht* (*BaFin*) haben 71 deutsche Erstversicherer im Jahr 2022 ein Prämienvolumen von ca. 700 Mio. € gezeichnet, wovon 336,1 Mio. € auf in Deutschland belegenes Geschäft entfiel. 15 deutsche Versicherer betrieben im selben Jahr die Cyber-Rückversicherung und erzielten weltweit ein Beitragsvolumen von 1,57 Mrd. €. Die Cyberversicherung ist stark von industrieller Kundschaft geprägt; so stammten ca. 80 % des Geschäftsvolumens von Industrieunternehmen, zwischen 15 % und 20 % von KMU und lediglich ca. 1 % von Privatkunden (vgl. *BaFin*, 2024).

Ihre **historischen Anfänge** findet die „moderne" Cyberversicherung in der Computer-Missbrauch-Versicherung und der Datenmissbrauch-Versicherung, die in den 1970er und 1980er Jahren etabliert wurden (vgl. *Koch*, 2024, S. 13 f.). Die Gefahrenlagen bestanden damals vor allem aus Computerkriminalität durch eigene Mitarbeiter oder durch Dritte, was aufgrund der noch nicht existenten Vernetzung unmittelbaren Zugriff auf die Geräte erforderte. Zudem stellten Computer und Datenträger wirtschaftliche Werte an sich dar. Deren Beschädigung konnte ab 1976 durch eine Datenträger- und Datenversicherung abgesichert werden, reiner Datenverlust später durch eine Software-Versicherung. Mit der Popularisierung des Internets und der zunehmenden Vernetzung von IT-Systemen entwickelten sich weitere Absicherungsbedürfnisse, z.B. gegen Hacker-Angriffe, Denial-of-Service-Attacken und Angriffen mittels Schadsoftware (vgl. *Koch*, 2024, S. 15; *Gordon/Loeb/Sohail*, 2003, S. 82). Auch Haftpflichtdeckung für Software-Häuser, Internet-Provider sowie Hardwarehersteller und -händler wurde angeboten, genauso wie Entschädigungen bei rechtswidrigen Eingriffen in die elektronische Datenverarbeitung aufgrund von zielgerichteten Angriffen gegen den Versicherungsnehmer sowie Betrugsschäden durch Cybercrime. Die ersten umfassenden Cyberversicherungen, die sich ohne wesentliche Einschränkungen auf IT-Eigen- und Fremdschäden erstreckten, wurden Anfang der 2010er Jahre angeboten. Seit 2017 ist zudem die Einbeziehung von Lösegeldzahlungen nach Ransomware-Attacken üblich.

Die zunehmende Erweiterung der versicherten Gefahren, aber auch die verstärkte öffentliche Wahrnehmung von Cybergefahren ließ vor allem in der zweiten Hälfte der 2010er Jahre die Prognosen zu Marktanteilen der Cyberversicherung rapide in die Höhe schnellen. Erwartungen sahen die Cyberversicherung in naher Zukunft betragsmäßig auf Höhe der Kfz-Versicherung (vgl. *KPMG*, 2017, S. 38). Derartige Prognosen haben sich jedoch (noch) nicht bewahrheitet, was auch auf gewisse Zurückhaltung der Anbieter zurückzuführen ist, die aufgrund von stark ansteigenden Schadenfällen zunahm. Zudem hängt der Erstversicherungsmarkt im Cyberversicherungsbereich außergewöhnlich stark vom Risikoappetit und der Risikotragfähigkeit des weltweiten – und letztlich auch noch konzentrierten – **Rückversicherungsmarktes** ab. Während im Sach- und Haftpflichtversicherungsbereich üblicherweise 10 % bis 15 % der Prämien an Rückversicherer zediert werden, beträgt das Volumen im Cyberversicherungsbereich Schätzungen zufolge bis zu 50 % (vgl. *Pain*, 2024, S. 10). Verknappung des Cyberversicherungsangebots und entsprechend restriktive Konditionen veranlassten europäische Industriekonzerne sogar dazu, Ende 2022 eine eigene Cyberversicherungsgesellschaft zu gründen, die *Mutual Insurance and Reinsurance for Information Systems (MIRIS)* mit Sitz in Brüssel, die ausschließlich ihren Mitgliedern nach einem umfangreichen Prüfungsverfahren Versicherungsdeckung gewährt (vgl. *MIRIS*, 2025).

3.2. Inhalte der Cyberversicherung

Aufgrund der verschiedenen Gefahren, die in der Cyberversicherung zusammengefasst sind, wie beispielsweise verschiedene finanzielle Verluste bei Eigenschäden, aber auch Schadenersatz aufgrund von Haftpflicht, gilt sie als **verbundene Versicherung**, deren Bedingungen in einem Vertrag zusammengefasst werden (vgl. *Koch*, 2024, S. 12), was wiederum ihre Komplexität begründet.

In den Bedingungen der Cyberversicherungsprodukte werden nicht alle denkbaren Gefahren rund um Cyberrisiken abgesichert. Vielmehr sind Positivlisten üblich, in denen benannt wird, welche Eigen- und Fremdschäden (vgl. hierzu *Biener/Eling/Matt/Wirfs*, 2015, S. 10) aufgrund von Informationssicherheitsverletzungen auf Basis welcher Ursachen (versicherte Gefahren) versichert werden. Üblicherweise finden sich auch sog. **Assistance-Leistungen** inkludiert, beispielsweise forensische Dienstleistungen im Falle eines Hacker-Angriffs oder Leistungen von Drittdienstleistern bei notwendiger Datenwiederherstellung (vgl. *Tsohou* et al., 2023, S. 744). Das Spektrum reicht hier bis hin zu Vermittlungsleistungen zwischen Betroffenen und Cybererpressern.
Neben den inhaltlichen Einschränkungen werden **Limite** bei den Versicherungssummen gesetzt, genauso wie Selbstbehalte oder Wartezeiten. Aufgrund der jüngeren Schadenerfahrungen haben Versicherer ihre maximalen Versicherungssummen abgesenkt, so dass sich diese für den industriellen Bereich bei ca. 10 Mio. € bewegen (vgl. *Koch*, 2024, S. 18).
Für Versicherungsnehmer werden gefahrvorbeugende Pflichten, sog. **Obliegenheiten**, definiert, die das vom Versicherer übernommene Risiko berechenbar halten sollen. Andernfalls droht die Gefahr, dass nach Abschluss einer Cyberversicherung weitere, nicht zwingend umzusetzende Maßnahmen zur Schaffung von Cybersecurity unterlassen bzw. eingestellt werden. Solche Obliegenheiten beziehen sich vor allem auf ein Mindestniveau an Schutzmaßnahmen, wie beispielsweise Regelungen zu Passwörtern und Datei- und Netzwerkzugriffrechten, Virenschutz, Installation von Sicherheitsupdates und Zahl sowie Häufigkeit von Sicherheitskopien essenzieller Daten. Auch die umgehende Anzeige von Gefahrerhöhungen oder Gefahränderungen zählen zu den Obliegenheiten.

3.3. Alternativer Risk Transfer: Cyber Bonds

Neben „klassischen" Versicherungsverträgen, in denen Erst- und Rückversicherer als Risikoträger fungieren, werden seit kurzem auch Instrumente des alternativen Risikotransfers genutzt, um Cyberrisiken zu versichern und die Kapazitätsengpässe auf dem weltweiten (Rück-)Versicherungsmarkt abzumildern. Zu den **Insurance-Linked Securities** (vgl. *Pain*, 2024, S. 15 ff.) zählen sog. Cat Bonds, eine Wertpapierkategorie, bei der Zins- und Tilgungszahlungen an den Nicht-Eintritt eines in den Anleihebedingungen festgelegten Schadenereignisses gekoppelt sind. Tritt das Ereignis hingegen ein, müssen Investoren auf Zins- und meist auch auf anteilige oder komplette Tilgungsleistungen verzichten (vgl. *Hartung*, 2004). Cyber Insurance-Linked Securities oder **Cyber Bonds** nutzen diese Grundkonstruktion, um Cyberrisiken auf Investoren zu übertragen (vgl. *Braun/Eling/Jaenicke*, 2023). Insurance-Linked Securities, die vor allem Naturkatastrophenrisiken auf den Kapitalmarkt transferieren, umfassen inzwischen ca. 15 % der weltweiten Rückversicherungskapazität. Anfang 2023 wurde vom Londoner Versicherer *Beazley* nach mehrjähriger Vorlaufzeit ein Cat Bond erstmalig genutzt, um ausschließlich Cyberrisiken in einer Anleihe zu verbriefen und auf Investoren zu übertragen. Sollten die Gesamtschäden aus einem Cyberangriff 300 Mio. US-Dollar übersteigen, werden die Investoren an den Schadenzahlungen beteiligt. Seitdem wurden weitere Cyber Bonds emittiert, die sich nicht nur auf Cyberattacken, sondern teilweise auch auf Schäden infolge des Ausfalls von Cloud-Infrastruktur beziehen (vgl. *Artemis*, 2025). Dennoch bewegen sich Cyber Bonds aktuell noch auf niedrigem Niveau und repräsentieren mit ihrer Deckungskapazität unter 2 % aller im Umlauf befindlichen Cat Bonds. Auf Investorenseite tragen noch zu gering entwickelte Marktstandards in den zugrunde liegenden Cyberversicherungsverträgen, relativ hohe Marktilliquidität und geringere mutmaßliche Diversifizierungsvorteile als bei NatCat Bonds zur Zurückhaltung bei (vgl. *Pain*, 2024, S. 29 ff.), auch wenn die gewährten Risikoprämien – auch aufgrund des Neuigkeitsgehalts des Finanzinstruments – weit überdurchschnittlich ausfallen.

4. Modellierung und Bewertung von Cyberversicherung

4.1. Modellierung der Cyberrisikoexponierung

Zur Verdeutlichung der **Risikoexponierung** werden Modelle genutzt, die eine Einbettung in Netzwerkstrukturen und die Kontrolle über darin befindliche Knotenpunkte widerspiegeln (vgl. *Böhme/Laube/Riek*, 2019, S. 170 f.). Erschwert wird eine Einschätzung der eigenen Exponierung dadurch, dass Cyberereignisse – ähnlich wie in Logistikketten – von vor- oder nachgelagerten Netzwerkknoten ausgehend sich über komplette Netzwerkstrukturen ausbreiten können oder Anfälligkeiten bei Standardkomponenten wie z.B. Netzwerkhardware oder Betriebssystemsoftware eine Vielzahl von Anwendern gleichzeitig betreffen. Zudem steht bedrohten Organisationen die Möglichkeit offen, durch Investitionen in **Sicherheitstechnologie** ex ante Cyberrisiken zu reduzieren.
Eine ökonomische Modellierung der Cyberrisikoexponierung kann in einem nutzentheoretischen Rahmen erfolgen. In einer vereinfachten Modellwelt wird dabei unterstellt, dass Schäden aus einem Cybervorfall in (fester) Höhe l und mit Wahrscheinlichkeit p eintreten können. Allerdings kann p beeinflusst werden, indem entsprechende Sicherheitstechnologie s – deren Wirkung durch die folgende „Abwehrfunktion" D repräsentiert wird – angewandt wird (vgl. *Böhme/Laube/Riek*, 2019, S. 172):

$p = D(s) = \beta^{-s}$, mit $\beta > 0$ als Parameter für die Wirksamkeit der Sicherheitstechnologie.

Aus Sicht eines gegenüber Cyberrisiken risikoavers eingestellten Unternehmens erfolgt die ökonomische Bewertung der Cyberrisikoexponierung mittels einer Nutzenfunktion u, die die Risikoaversion gegenüber Cyberrisiko repräsentiert. Wenn W das Endvermögen des Unternehmens nach Investition in Sicherheitstechnologie s darstellt, gilt unter der Annahme eines Anfangsvermögens in Höhe von w für den Erwartungsnutzen, abhängig vom Eintritt bzw. Nicht-Eintritt eines Cybervorfalls:

$$E[u(W_s)] = D(s) \cdot u(w - l - s) + (1 - D(s)) \cdot u(w - s)$$

Der Erwartungsnutzen des Unternehmens wird somit einerseits durch die Höhe der finanziellen Schäden aufgrund von Cybervorfällen, andererseits durch die Eintrittswahrscheinlichkeit solcher Ereignisse beeinflusst, wobei diese wiederum durch eine kostenbehaftete Sicherheitstechnologie reduziert werden kann.

4.2. Bewertung von Cyberversicherung aus Unternehmenssicht

Für ein Unternehmen gilt es nun, diesen **Erwartungsnutzen** zu maximieren, wenn neben der Investition in Sicherheitstechnologie zusätzlich der Abschluss eines Cyberversicherungsvertrags zur Verfügung steht:

$$\max_s \left(E[u(W_s)]\right)$$

Für das betreffende Unternehmen sei die Möglichkeit gegeben, bis zu einer Entschädigungshöchstgrenze $x < l$ Cyberversicherung zum Prämiensatz π (pro Geldeinheit Deckung) bzw. zur absoluten Prämie $\pi \cdot x$ zu erwerben. Das zu lösende Optimierungsproblem liefert die „idealen" Investitionen in Sicherheitstechnologie und Versicherungsschutz (vgl. *Böhme/Laube/Riek*, 2019, S. 172):

$$(s,x)^* = \arg\max_{s,x} D(s) \cdot u(w - l - s + (1 - \pi) \cdot x) + (1 - D(s)) \cdot u(w - s - \pi \cdot x)$$

Bereits ohne vertiefte Berücksichtigung versicherungsmarkttypischer Phänomene wie Informationsasymmetrien aufgrund von adverse selection oder moral hazard (vgl. *Gordon/Loeb/Sohail*, 2003, S. 82 f.) kann festgehalten werden, dass die Nachfrage nach Cyberversicherung von der Risikoaversion bedrohter Unternehmen und der exakten Form der Abwehrfunktion D abhängt. Je risikoaverser Unternehmen gegenüber Cyberrisiko eingestellt sind und je weniger wirksam Sicherheitstechnologie funktioniert, desto mehr Versicherungsschutz wird nachgefragt.

Versicherungsprämien enthalten neben dem Anteil, der rein für die Deckung und den Ausgleich des übernommenen Risikos vorgesehen ist, einen Zuschlag für die anfallenden Verwaltungskosten sowie einen Sicherheitszuschlag, der die finanzielle Stabilität des Versicherers sicherstellt. Entsprechend setzt sich der **Prämiensatz** π wie folgt zusammen:

$$\pi = D(s^*) \cdot (1 + \lambda)$$

Aus Unternehmenssicht ist die Prämie Bestandteil der **Total Cost of Risk (TCoR)**. Mit Hilfe dieser Kennzahl soll der risikobezogene Gesamtaufwand minimiert und ein optimales Verhältnis zwischen Risikoeigentragung und Risikotransfer bestimmt werden. Die TCoR lassen sich folgendermaßen ermitteln (vgl. *Kloman*, 1992, S. 300 f.):

TCoR = Versicherungsprämien
- \+ erwartete Eigenschäden (durch Selbstbehalte und/oder unversicherte Schäden)
- \+ Kosten des Risikokapitals (vorzuhaltendes Eigenkapital)
- \+ Präventionskosten
- \+ risiko(management)bezogener Administrations- und Kontrollaufwand

Die einzelnen Komponenten der TCoR stehen in einem Abhängigkeitsverhältnis zueinander. Umso höher beispielsweise Selbstbehalte gewählt und Cyberrisiko-Präventionsmaßnahmen getroffen werden, desto mehr Versicherungsdeckung kann abgeschlossen werden bzw. derselbe Deckungsumfang erfordert eine geringere Versicherungsprämie (vgl. *Gordon/Loeb/Sohail*, 2003, S. 84).

Eine weitere Besonderheit bei Cyberrisiken beruht darauf, dass die eigene Sicherheit nicht nur von eigenen Schutzmaßnahmen, sondern auch von den Schutzmaßnahmen anderer Akteure in einem Netzwerk beeinflusst wird. Eigene Investitionen in Sicherheitstechnologie lösen (positive) **Externalitäten** aus, da dadurch die Angriffsgefahr für das gesamte Netzwerk, also auch für Netzwerkknoten, die unter Kontrolle anderer am Netzwerk Beteiligter stehen, reduziert wird. Spieltheoretische Modellierungen, die das optimale Investitionsniveau in Sicherheitstechnologie s vor diesem Hintergrund ermitteln sollen, münden dann aber im wohlbekannten **Gefangenendilemma** und dem Ergebnis, dass das gesamtgesellschaftlich optimale Niveau an Investitionen aufgrund des Freerider-Problems unterschritten wird (vgl. *Böhme/Laube/Riek*, 2019, S. 174 f.). Vorgaben von Versicherern zum technologischen Mindestabsicherungsniveau oder regulatorischer Zwang können hier einen das Gefangenendilemma auflösenden Effekt bewirken.

4.3. Aktuarielle Bewertung von Cyberrisiken

Eine aktuarielle Bewertung von Cyberrisiken orientiert sich – wie häufig in versicherungstechnischen Fragestellungen der Fall – an der Eintrittswahrscheinlichkeit von Cyberereignissen und deren erwarteten (finanziellen) Folgen. Dies

setzt auskömmliche Bestände historischer **Ereignis-** bzw. **Schadendaten** voraus, die jedoch – wie empirische Befunde bestätigen (vgl. *Romanosky/Ablon/Kuehn/Jones*, 2019, S. 12 f.) – gerade im Fall der verhältnismäßig „jungen" Cyberrisiken häufig noch nicht in ausreichendem Umfang vorliegen. Anspruchsvoll wird die Erfassung des finanziellen Risikos zudem dadurch, dass unter dem Begriff des Cyberrisikos eben etliche verschiedene Schadenszenarien subsumiert sind, die alle mit unterschiedlichen Häufigkeiten und Schäden verbunden sind, möglicherweise aber gleichzeitig auftreten können. Hilfreich für entsprechende Risikomodelle sind daher Taxonomien der Bewertungsmodell-Kategorien sowie eine Zuordnung bislang entwickelter Cyberrisiko-Modelle dazu (vgl. hierzu *Bardopoulous*, 2025, S. 2).

Modelle zur Bewertung von Risiken und zur anschließenden Kalkulation einer auskömmlichen Versicherungsprämie setzen am **Gesamtschaden** an. Der Gesamtschaden S, bezogen auf eine Gruppe ähnlicher und voneinander unabhängiger Cyber-Risiken (Kollektiv), wird für einen abgegrenzten Zeitraum in der Risikotheorie anhand der Zufallsvariablen Schadenanzahl N und Schadenhöhe X_i modelliert (vgl. *Helten*, 2002, S. 46):

$$S = X_1 + X_2 + X_3 + \ldots + X_N$$

Zur Modellierung der (stochastischen) Anzahl von Cyberereignissen N bzw. der Wiederkehrperioden werden in den jeweiligen Modellen geeignete **Wahrscheinlichkeitsverteilungen** wie die Poisson- oder die Negative Binomialverteilung bzw. stochastische **Zählprozesse** verwendet. Beispiele hierfür sind der homogene Poisson-Prozess, der Pareto-Prozess, der Binomial-Prozess oder ein inhomogener Poisson-Prozess. Die Modellierung von Schadenhöhen X erfolgt teilweise unter der restriktiven Annahme konstanter Schäden, häufiger aber mit verschiedenen als passend erachteten Verteilungsmodellen, wie der Lognormal-, der Gamma-, der Pareto- oder der Weibull-Verteilung. Für die Modellierung des Tail-Verhaltens wird auch auf Modelle der Extremwerttheorie zurückgegriffen (vgl. *He* et al., 2024, S. 285 ff.). Sofern vorhanden, werden alternativ direkt statistische Parameter der Daten aus zugrundeliegenden Cyber-Schadendatenbanken verwendet (vgl. *Bardopoulous*, 20025, S. 3; *Braun/Eling/Jaenicke*, 2023, S. 693 f.). Für die Ermittlung des Gesamtschadens S besteht regelmäßig die Herausforderung, dass dieser nur unter einschränkenden Annahmen bezüglich der verwendeten Wahrscheinlichkeitsverteilungen für die X_i in einer geschlossenen Form darstellbar ist, da dann das sogenannte n-fache Faltungsprodukt der Schadenhöhenverteilung berechnet werden kann. In allen anderen Fällen ist auf **Approximationen** oder numerische Verfahren zurückzugreifen, wie beispielsweise Rekursionsverfahren, die Fast-Fourier-Transformation, Monte-Carlo-Simulationen o.ä. (vgl. *Cottin* et al., 2025, S. 100 f.; *Shevchenko*, 2010).

Das bedeutendste Hemmnis für die Versicherungsproduktgestaltung, die Prämienkalkulation und die versicherungsbetriebliche Risikopolitik besteht im Fehlen der oben unterstellten **Unabhängigkeit** der Risiken in einem Cyber-Kollektiv. Von einzelnen Cybervorfällen können etliche Versicherungsverträge gleichzeitig betroffen sein, sodass die für Versicherer bedeutsamen Gesetze der großen Zahlen nur eingeschränkt wirken. Zur Modellierung eignen sich dann Ansätze, die nicht-lineare Abhängigkeiten abbilden können, wie beispielsweise Copulas (vgl. *He* et al., 2024, S. 283 ff.). Versicherungstypische Maßnahmen zur Abhilfe sind Ausschlüsse bestimmter Schadenereignisse, Zeichnungslimite, Prämienzuschläge und – im Falle der Cyberversicherung besonders bedeutsam – Rückversicherungsnahme.

Eine Systematik bei der Bewertung folgt der in den Versicherungsverträgen vorzufindenden Einteilung nach Eigenschäden, Fremdschäden und Assistance-Leistungen. Die konkreten Schadenszenarien, wie zum Beispiel die Beschädigung der IT-Infrastruktur aufgrund eines Hacker-Angriffs mit anschließender temporärer Betriebsunterbrechung oder der Abfluss personenbezogener Daten im Rahmen von Cybercrime, werden in die jeweiligen Kategorien einsortiert und dann mittels versicherungsmathematischer Verfahren Schätzungen der zu erwartenden Versicherungsleistungen errechnet. Dabei kann zwischen meist häufiger eintretenden, aber mit möglicherweise geringeren finanziellen Belastungen verbundenen Eigenschäden und selteneren, aber hohes Schadenpotenzial aufweisenden Haftpflichtschäden gegenüber Dritten unterschieden werden. Allerdings treten auch Schadenszenarien nicht unabhängig voneinander auf, sodass Annahmen zu **Interdependenzen** berücksichtigt werden müssen, basierend auf historischen Daten oder Szenarioanalysen. Beispielsweise betreffen Cyberangriffe, die zu Datenabfluss und anschließender Verschlüsselung sowie nachfolgenden Erpressungen hinsichtlich der Veröffentlichung von Daten Dritter führen, sowohl die Kategorie der Eigen- als auch der Fremdschäden. Dazu werden regelmäßig Asssistance-Leistungen in Anspruch genommen, wenn beispielsweise versucht wird, Daten ohne Lösegeldzahlung wieder herzustellen oder letztlich Verhandlungen mit Cybererpressern geführt werden.

Zudem drohen kaum bewertbare **Kumulrisiken** aufgrund der omnipräsenten weltumspannenden Nutzung des Internets bei gleichzeitig nur wenigen die Zugänge bereitstellenden Internet Service Providern (ISP) und ebenso wenigen die Betriebssysteme für Computer anbietenden Unternehmen.

Die jährlichen **Versicherungsprämien** werden dann anhand derjenigen Risikomerkmale differenziert, die mutmaßlich den größten Einfluss auf die Schadenhöhe aus-

üben. In konkreten Cyberversicherungspolicen wurden hierfür der jährliche Umsatz, das Gesamtvermögen, die Branchenzugehörigkeit, die Antworten im Risikofragebogen und vereinzelt auch die Mitarbeiterzahl identifiziert. Weitere Tarifmerkmale umfassen die Zahl und/oder Höhe vergangener Schäden, die Vertragslaufzeit oder die Einbeziehung von Betriebsunterbrechungen. Höchstversicherungssummen und Selbstbehaltsvereinbarungen wirken ebenfalls auf die kalkulierte Prämie ein (vgl. *Romanosky/Ablon/Kuehn/Jones*, 2019, S. 15 ff.).

5. Fazit

Cyberrisiken gelten als die mitunter am dynamischsten sich entwickelnde Risikokategorie. Unter Versicherungsaspekt ist mit einer erheblichen Ausweitung des Marktvolumens zu rechnen, auch wenn frühere Prognosen nicht in der prophezeiten Geschwindigkeit eingetreten sind. Dazu gilt es, Hindernisse für die Marktentwicklung zu beseitigen. Dazu gehören die Schaffung einheitlicher Begriffsverständnisse, welche Ereignisse unter die Definition von Cyberrisiken fallen, eine fortschreitende Standardisierung von Versicherungsbedingungen, eine effiziente(re) Erfassung und Bewertung von Risikoexposures bei Kunden, die Schaffung von Datengrundlagen zur Risikobewertung und Prämienbemessung sowie die Entwicklung von fortgeschrittenen Verfahren des Machine Learnings zur Entdeckung und Abwehr von Cyberangriffen.

Literatur

Allianz Commercial/Allianz Global Corporate & Specialty SE, Allianz Risk Barometer: Identifying the major business risks for 2026, München 2026.

Artemis, Artemis Deal Directory, Online, URL: https://www.artemis.bm/deal-directory/?_sft_perils=cyber-risks

BaFin, Cyberversicherungen: hohe Nachfrage – und hohe Risiken, in: BaFin-Journal vom 7.2.2024, Online, URL: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2024/fa_bj_2402_Cyberversicherung.html.

Bardopoulous, J., Cyber-insurance pricing models, in: British Actuarial Journal, Vol. 30 (2025), S. 1–31.

Biener, C., Eling, M., Matt, A., Wirfs, J. H., Cyber Risk: Risikomanagement und Versicherbarkeit, Institut für Versicherungswirtschaft der Universität St. Gallen 2015.

Böhme, R., Laube, S., Riek, M., A Fundamental Approach to Cyber Risk Analysis, in: Variance Vol. 12 (2019), No. 2, S. 61–85.

Braun, A., Eling, M., Jaenicke, C., Cyber insurance-linked securities, in: Astin Bulletin, Vol. 53 (2023), S. 684–705.

Cottin, C., Döhler, S., Schmidt, J.-P., Risikoanalyse: Modellierung, Beurteilung und Management von Risiken mit Praxisbeispielen, 3. Aufl., Wiesbaden 2025.

Drefke, G., Der CrowdStrike-Vorfall – ein Warnschuss für Versicherer?, Online, URL: https://www.genre.com/int/knowledge/publications/2025/february/the-crowdstrike-incident-a-wake-up-call-for-insurers-de#accordion-b7096a674f-item-352150d21c.

DSGVO-Portal.de (2026): Sicherheitsvorfälle, Online, URL: https://www.dsgvo-portal.de/sicherheitsvorfall-datenbank.

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

Hartung, T., Alternative Risikotransfer-Instrumente, in: WiSt – Wirtschaftswissenschaftliches Studium, 33. Jg. (2004), Nr. 4, S. 401–405.

He, R., Zhuo, J., Li, J. S.-H., Modeling and management of cyber risk: a cross-disciplinaryreview, in: Annals of Actuarial Science, Vol. 18 (2024), S. 270–309.

Helten, E., Stochastische Grundlagen, in: *Helbig, M.* (Hrsg), Beiträge zum versicherungsmathematischen Grundwissen, 2. Aufl., Karlsruhe 2002, S. 11–49.

Hunziker, S., Trachsel, V., Cyber-Risiken in das Risikomanagement integrieren, in: Controlling & Management Review, 67. Jg (2023), Nr. 2, S. 26–33.

IBM, Cost of a Data Breach Report 2025: Die Lücke bei der KI-Aufsicht, Zusammenfassung, 2025.

Kloman, H. F., Rethinking Risk Management, in: The Geneva Papers on Risk and Insurance, Vol. 17 (1992), S. 299–313.

Koch, R., Aktuelle Entwicklungen in der Cyberversicherung, in: Zeitschrift für die gesamte Versicherungswissenschaft, 113. Jg. (2024), Nr. 1, S. 11–53.

KPMG, Neues Denken, Neues Handeln: Insurance Thinking Ahead, Versicherungen im Zeitalter von Digitalisierung und Cyber, Studienteil B: Cyber, 2017.

Mutual Insurance and Reinsurance for Information Systems (MIRIS), FAQ, Online, URL: https://www.miris-insurance.com/en/faq.

Pain, D., Catalysing Cyber Risk Transfer to Capital Market: Catastrophe bonds and beyond, The Geneva Association, Zürich 2024.

Romanosky, S., Ablon, L., Kuehn, A., Jones, T., Content analysis of cyber insurance policies: how do carriers price cyber risk?, in: Journal of Cybersecurity, Vol. 5 (2019), No. 1, S. 1–19.

Shevchenko, P. V., Calculation of aggregate loss distributions, in: The Journal of Operational Risk, Vol. 5 (2010), No. 2, S. 3–40.

Tsohou, A., Diamantopoulou, V.,Gritzalis, S., Lambrinoudakis, C., Cyber insurance: state of the art, trends and future directions, in: International Journal of Information Security, Vol. 22 (2023), S. 737–748.

Zängerle, D., Schiereck, D., Cyberrisiken – Vom Begriffswirrwarr zu einem einheitlichen Begriffsverständnis, in: HMD, 60. Jg. (2023), S. 214 – 229.