Zeitschrift für die gesamte Versicherungswissenschaft, 114 (2025) 2: 199 – 225
https://doi.org/10.3790/zverswiss.2025.1459203

# Cyber-Versicherungsnachfrage im KMU-Bereich

*Niklas Alexander Anders*

## Zusammenfassung

Cyberrisiken werden in der heutigen Zeit zunehmend relevanter. Unternehmen, Privatpersonen und staatliche Organisation sind vor einem Cyberangriff nicht mehr sicher geschützt. Versicherungsunternehmen zeichnen diese Risiken. Für das Zeichnen der Risiken ist das Zusammenspiel von Cyber-Risikomanagement und Cyberversicherung von großer Bedeutung. Gerade bei kleinen und mittelständischen Unternehmen (KMU) sind deutliche Defizite sichtbar. Die Nachfrage für eine Cyber-Versicherung ist bei KMU aktuell noch verhalten, obwohl Behörden und Versicherungsunternehmen die Bedeutsamkeit einer Cyber-Versicherung betonen. Hier stellt sich die Frage, welche Gründe es für die verhaltende Nachfrage gibt und wie diese behoben werden können. Mithilfe einer systematischen Literaturrecherche und diversen Experteninterviews soll diese Problematik aufgeklärt werden.

Dabei wird anhand einer Literaturrecherche die derzeitige Marktlage und Problemstellung erkennbar. Anschließend werden die Ergebnisse in Experteninterviews diskutiert, um sie zu verifizieren und weitere Lösungsansätze zu erarbeiten. Vorab wurden die Experten in drei Gruppen unterteilt, um unterschiedliche Sichtweisen besser herauszuarbeiten.

Die qualitative Studie führt zu folgenden Ergebnissen: Die Fragebögen für die Risikoerhebung sind gekennzeichnet von mangelnder Standardisierung, fehlender Transparenz und Verständnisschwierigkeiten. Weiterhin sind bereits abgeschlossene Verträge intransparent und weisen keine Qualitätsstandards aus, wie z. B. Zertifizierungen der IT-Forensiker. Außerdem ist für die Cyberversicherungen ein innovatives Deckungskonzept zu erarbeiten, um die Tragfähigkeit der Versicherungsunternehmen zu gewährleisten. Dabei ist auch das Gap zwischen dem Allgemeinen- und Individuellen Risiko der Geschäftsführer und dem Versicherungsvertrieb besonders zu beachten.

Niklas Alexander Anders
Universität zu Köln
Seminar für ABWL, Risikomanagement und Versicherungslehre
E-Mail: niklas.anders@uni-koeln.de


Duncker & Humblot · Berlin

**Abstract**

Cyber risks are increasingly relevant for companies, private individuals and government organizations. Insurance companies assume these risks, whereby the interaction between cyber risk management and cyber insurance is crucial. Small and medium-sized enterprises (SMEs) in particular have deficits, and although authorities and insurers point out the importance of cyber insurance, demand among SMEs is still low. A systematic literature review and expert interviews were conducted to investigate the reasons for this reluctance. The results show that the risk assessment processes lack standardization and transparency and that concluded contracts do not contain clear quality standards. In addition, an innovative coverage concept is needed to ensure the sustainability of insurers. There is a particular focus on the gap between the general and individual risks of managing directors and insurance sales. The study provides valuable insights and solutions for the optimization of cyber insurance and its demand.

*JEL classification:* D81, D85, G22, G32, L11, L86, M15, O33

*Keywords:* Cyber-Versicherung, Cyber-Versicherung im KMU-Bereich, Cyber-Risikomanagement, Optimierung der Cyber-Versicherung

## 1. Ausgangssituation und Problemstellung

Cyberrisiken zählen weltweit zu den größten Bedrohungen für Wirtschaft und Gesellschaft (Wrede, 2018). Die daraus resultierenden Cyberangriffe stellen eine erhebliche Bedrohung für verschiedene Sektoren dar, darunter Verkehr, öffentliche Dienstleistungen, Unternehmen und Finanzinstitute. Der Ursprung von Cyberrisiken kann hauptsächlich durch die Entwicklung und Verbreitung des Internets und dem Zuwachs von Nutzern, wie Unternehmen und Privatpersonen, im World Wild Web (WWW) erklärt werden (Njegomir, 2012). Ein häufig genannter Grund für die vermehrten Cyberangriffe, ist der weltweite Anstieg der Social-Engineering-Attacken, bei denen Cyberkriminelle die Mitarbeiter von fremden Unternehmen manipulieren, um Zugang zu deren IT-Systemen und Daten zu erhalten (Pfeiffer, 2021). Aber auch andere Bedrohungen, wie Identitätsdiebstahl durch Phishing, Datendiebstahl, Hackerangriffe oder Cyber-Mobbing sind sehr weit verbreitet, wie eine Studie der GDV zeigt (GDV, 2020). Versicherer können heutzutage Risiken von Cyber-Attacken, Datenverlust und Spionage zeichnen (Choudhry, 2014). Die Prämienkalkulation für eine solche Versicherung ist derzeitig jedoch noch problematisch. Neben zurechenbaren Kosten, wie defekte Hardware oder Betriebsausfälle – welche einfach zu erfassen sind – gibt es auch nicht messbare Kosten wie z. B. Reputationsverluste (Christian Biener, 2015). Auch Europa hat diese Gefahr erkannt und gegen die wachsende Bedrohung Maßnahmen ergriffen. So werden die Mitgliedsstaaten aufgefordert im Bereich Cybersicherheit ihre Zusammenarbeit und Investitionen zu verstärken (EP, 2022). Die immer häufiger aufkommenden Cyberattacken hat

die EU sensibilisiert, weshalb sie zukünftig eine führende Kraft beim Thema Cybersicherheit sein möchte (EP, 2022). Dazu hat sie eine neue Richtlinie beschlossen – die NIS 2.0 (BSI, 2022).

Durch datenschutzbezogene Pflicht- und Vertraulichkeitsverletzungen, Betriebsunterbrechungen, sowie Datendiebstahl können Reputationsverluste für Unternehmen als schwerwiegende Konsequenz aus Cyberangriffen folgen (Cavusoglu, 2004) (Smith, 2004). Die Schäden einer solchen Cyberattacke können existenzbedrohend sein (Petermann, 2021). Dies sollte unmittelbar zu einer hohen Nachfrage von Cyber-Versicherungen führen. Wie sich herausgestellt hat, gibt es noch erhebliche Defizite bei kleinen und mittelständischen Unternehmen, denn nur 13 % von ihnen besitzen eine Cyber-Versicherung (BaFin, 2020). Fraglich ist, warum bei einem existenzbedrohenden Risiko KMU selten dagegen versichert sind.

In der Literatur wird seitens KMU die mangelnde Dringlichkeit und das fehlende Interesse an der Sicherung von Daten gesehen (Hoppe, 2021). Durch Gesetze wie die DSGVO, oder auch Richtlinien wie die NIS 2.0, gibt es jedoch eine Zwangssensibilisierung für KMU. In dieser Arbeit wird daher davon ausgegangen, dass die geringe Anzahl an versicherten kleinen und mittelständischen Unternehmen, durch mehr Faktoren als nur die Dringlichkeit und das Interesse beeinflusst wird. Deshalb muss hier der Cyber-Versicherungsmarkt tiefer beleuchtet werden, um eine ganzheitliche Analyse durchführen zu können. Nur so besteht die Möglichkeit kritische Faktoren zu identifizieren. Um die Nachfrage von KMU im Cyber-Versicherungsmarkt herauszufinden, werden mehrere Betrachtungsgegenstände beleuchtet. Dazu werden in der vorliegenden Arbeit Versicherungsunternehmen, KMU und Rahmenbedingungen (Gesetzeslagen und IT-Dienstleister) näher analysiert. Dies ergibt einen ganzheitlichen Überblick des Cyber-Versicherungsmarkts und liefert Erkenntnisse über die derzeitigen Herausforderungen des Marktes.

Zusammenfassend besteht in der Literatur Einigkeit über die Existenzbedrohung durch Cyberrisiken und das Cyber-Versicherungen einen guten Schutz vor finanziellen Schäden bieten. Da jedoch nur eine geringe Anzahl von KMU über diesen Versicherungsschutz verfügen, stellt sich die Frage, warum der Cyber-Versicherungsmarkt, trotz erheblicher Relevanz für KMU sehr verhalten ist, und welche Strategien sich hieraus ableiten lassen.

Die vorliegende Arbeit soll einen Beitrag zur Schließung dieser Forschungslücke leisten. Ziel ist es, Gründe für die verhaltende Nachfrage von Cyberversicherungen durch KMU zu ermitteln und mögliche kritische Faktoren seitens der Versicherer aufzuzeigen, um passende Lösungsstrategien zu entwickeln. Dazu wird in Abschnitt 2 zunächst eine begriffliche Einordnung und Abgrenzung des Terminus Cyberrisiken und KMU vorgenommen. Weiterführend wird in Abschnitt 3 ein Überblick bezüglich der relevanten Literatur zur Marktent-

wicklung von Cyber-Versicherungen im Bereich KMU gegeben. Abschnitt 4 handelt von der Methodik und beschreibt das Forschungsdesign, sowie die Vorgehensweise bei der Datenerhebung und -auswertung. In Abschnitt 5 werden die Ergebnisse der analysierten Experteninterviews dargestellt. Eine entsprechende Diskussion der erarbeiteten Ergebnisse ist Gegenstand von Abschnitt 6. Abschließend befindet sich in Abschnitt 7 eine kurze Zusammenfassung der Ergebnisse nebst Schlussfolgerungen.

## 2. Begriffsdefinition und Abgrenzung

Kleine und mittlere Unternehmen (KMU) sind ein wichtiger Teil der Weltwirtschaft, allerdings gibt es keine allgemein anerkannte Definition. Verschiedene quantitative und qualitative Variable wurden vorgeschlagen, um unterschiedliche Aspekte von KMU zu messen, aber es gibt keine einheitliche Lösung die für alle Zwecke geeignet ist (Dyah, 2023). Tab. 1 veranschaulicht die verschiedenen Definitionen. In dieser Arbeit gilt ein Unternehmen als KMU, wenn es maximal 249 Mitarbeiter beschäftigt, einen Umsatz unter 50 Millionen Euro tätigt, oder über eine Bilanzsumme bis 43 Millionen Euro verfügt (Bonn, 2003). Werden zwei der drei Merkmale überschritten, gilt es in dieser Ausarbeitung nicht mehr als KMU.

*Tabelle 1*

**Überblick über gängige Definitionen von KMU anhand quantitativer Merkmale (in Anlehnung an (Behringer, 2012))**

| Institution bzw. Gesetz | Definition KMU |
|---|---|
| §267 Abs. 2 HGB; Grenze für mittelgroße Kapitalgesellschaften | Bilanzsumme < 19,25 Mio. EUR pro Jahr;<br>Umsatz < 28,5 Mio. EUR pro Jahr;<br>Arbeitnehmer im Jahresdurchschnitt < 250<br>(zwei Kriterien dürfen an zwei aufeinander folgenden Bilanzstichtagen nicht überschritten werden, damit die Schwelle zur mittelgroßen Kapitalgesellschaft nicht erreicht wird) |
| Statistisches Bundesamt | < 250 Beschäftigte und Jahresumsatz < 50 Mio. EUR (Destatis, 2024) |
| Empfehlungen der EU-Kommission betreffend die kleinen und mittleren Unternehmen | < 250 Beschäftigte, Jahresumsatz < 50 Mio. EUR oder Bilanzsumme < 43 Mio. EUR (Bonn, 2003) |
| Deloitte Mittelstandsforschung an der Universität Bamberg | < ca. 3.000 Mitarbeiter und < ca. 600 Mio. EUR Jahresumsatz (Becker, 2008) |

| Institution bzw. Gesetz | Definition KMU |
|---|---|
| Beratungsförderung des Bundes | Es gilt die empfohlene Definition der EU-Kommission (Völz, 2018) |
| Bundesverband mittelständischer Wirtschaft, Bonn | Jahresumsatz ≤ 50 Mio. EUR und Beschäftigungszahl < 500 Mitarbeiter (BAFA, 2012) |

In der bestehenden wissenschaftlichen Literatur wird häufig eine Differenzierung zwischen Informationssicherheits- und IT-Risiken, sowie Cyberrisiken vorgenommen. Während unter dem Begriff Informationssicherheitsrisiken alle Abweichungen von den allgemeinen Schutzzielen der IT-Sicherheit, der Vertraulichkeit, Integrität und Verfügbarkeit zusammengefasst sind (Königs, 2017), werden unter dem Begriff IT-Risiken alle aus dem Einsatz von IT resultierenden Bedrohungen verstanden (Seibold, 2006).

Auch Cyberrisiken sind in der wissenschaftlichen Literatur nicht klar definiert und werden daher nicht einheitlich abgegrenzt. Somit findet sich in der Literatur eine Vielzahl unterschiedlicher Cyberrisiken, die begrifflich eng, oder auch weit gefasst sind. Einen Überblick der ausgewählten Literatur des Begriffs Cyberrisiken gibt Tab. 2.

*Tabelle 2*

**Ausgewählte Definitionen des Begriffs Cyberrisiken**

| (Autor, Jahr) | Begriffsdefinition |
|---|---|
| (Mukhopadhyay, 2013) | „Risk involved with malicious electronic events that cause disruption of business and monetary loss“ |
| (Cebula, 2014) | „Operational risks to information and technology assets that have consequences affectiong the confidentiality, availability, or integrity of information or information systems“ |
| (Hiller, 2013) | „A company's cyber risk is a function of threats, vulnerabilities, the cybersecurity environment, and company-specific mitigation“ |
| (Eling M. S., 2016) | „Any risk emerging from the use of information and communication technology (ICT) that compromises the confidentiality, availability, or integrity of data or services. The impairment of operational technology (OT) eventually leads to business disruption, (Critical) infrastructure breakdown, and physical damage to humans and property“ |

*(Fortsetzung nächste Seite)*

*(Fortsetzung Tabelle 2)*

| **(Autor, Jahr)** | **Begriffsdefinition** |
|---|---|
| (Ruan, 2017) | „Cyber risk is the likelihood of economic loss from cyber incidents“ |
| (Haas, 2014) | „Risiken, die im Zusammenhang mit der Verarbeitung von digitalen Informationen stehen und somit auch auf das Cloud-Computing zutreffen, werden als Cyberrisiken bezeichnet“ |
| (Oğüt, 2011) | „Information security risk“ |

Die zentrale Eigenschaft von Cyberrisiken zeigt, dass es hoch korrelierte und globale Risiken sind, welche sowohl einen kurzfristigen als auch langfristigen Zeithorizont aufweisen und aus denen Eigen- und Fremdschäden resultieren können (Eling M. W., 2016). Cyberrisiken differenzieren sich durch verschiedene Merkmale: Angriffsformen (z. B. Spam, Distributed Denial of Service (DDoS)-Attacken, Insider-Angriffe und Schadsoftware), Aktivitäten (nicht kriminelle und kriminelle Handlungen), sowie Verursacher (Cyberterroristen, Cyberkriminelle und staatliche Institutionen) (Eling M. S., 2016).

Zudem kann weitergehend zwischen alltäglich stattfindenden – von Cyberkriminellen verursachten Einzelangriffen – und aus Cyberbedrohungen resultierenden Extremszenarien unterschieden werden. Zwar besteht trotz des erheblichen Bedrohungspotenzials eine Versicherung für gezielte Einzelangriffe, jedoch gelten cyberbezogene Extremszenarien, durch das nicht abschätzbar zu erwartende Schadensausmaß, i. d. R. mit den bestehenden Versicherungskapazitäten als nicht versicherbar (Eling M. W., 2016).

Hieraus lässt schließen, dass für den Begriff „Cyberrisiken“ im Schrifttum keine einheitliche Definition existiert. Um Cyberrisiken also genau zu definieren, müssen Versicherungsunternehmen eine klare Abgrenzung durchführen und diese auch mit dem Versicherungsnehmer kommunizieren.

## 3. Literaturüberblick

Aus der Literatur ist ersichtlich, dass bereits mehrfach in den Bereichen der Versicherbarkeit von Cyberrisiken und auch Cyber-Versicherungen als Instrument des Risikomanagements geforscht wurde. Die Versicherung von Internetrisiken wurde aus verschiedenen Perspektiven der Akteure des WWW (Anderson, 1994; Blind, 1996; Lesch, 2000; Grzebiela, 2002) bereits Anfang der 2000er Jahre erforscht, wohingegen Cyberpolicen und deren Einbindung in das Risikomanagement erst später erforscht wurden und auch heute immer noch weiter

erforscht werden (Biener, 2015; Tosh, 2017; Chen, 2022; Romanosky S. S., 2023; Tsohou, 2023).

In der Literatur wird die Cyber-Versicherung als Instrument des Risikomanagements gesehen (Soyer, 2023). Weitere Untersuchungen galten den Unsicherheitsfaktoren, welche bei Unternehmen im Umgang mit neuen Cyber-Versicherungsprodukten vorhanden sind (Meland, 2017). Da bei Cyberattacken erhebliche Schäden aufkommen können, ist die Gewährleistung der IT-Sicherheit für Unternehmen von größter Bedeutung. Folglich resultiert daraus, dass es für die Unternehmensführung ein wichtiges Ziel ist, diese auch zu gewährleisten (Brancheau, 1996; Kankanhalli, 2003; Ransbotham, 2009; Luftman, 2010). Während der Verantwortungsbereich für die Cybersicherheit in KMU nicht klar definiert ist (Katkova, 2020), binden große Unternehmen die IT-Sicherheit sehr stark in ihr Geschäftsziel ein. Sie sind damit auch eher bereit eine Cyber-Versicherung abzuschließen, wobei KMU oftmals darauf verzichten (Soyer, 2023). Als Grund wird hier die fehlende Dringlichkeit, sowie mangelndes Interesse erwähnt (Hoppe, 2021; Abhilash, 2023). Deshalb stellen die eigenen Mitarbeiter und deren Verhalten eine wichtige Herausforderung für Unternehmen dar, da sie ein relevantes Risiko für die IT-Sicherheit sind (Bauer, 2009; Lebek, 2014).

Spätestens mit den neuen Richtlinien NIS 2.0 (BSI, 2022) müssen sich jedoch auch KMU mit dieser Thematik beschäftigen. Die deutsche Regierung wird bis Ende 2024 einen neuen Gesetzesentwurf herausbringen, an dem sich natürlich auch KMU halten müssen (BSI, 2022). Die Bedeutung einer Cyber-Versicherung für Unternehmen im Rahmen eines umfassenden Cyber-Risikomanagement wird häufig in der wissenschaftlichen Literatur betont (Böhme, 2006; Faisst, 2007). Ebenso wird in diesem Zusammenhang vermehrt diskutiert, wie Cyber-Policen Unternehmen bei der Unterstützung ihrer bereits ergriffenen IT-Sicherheits- und Schutzverfahren unterstützen (Siegel, 2002; Gordon, 2003). Es werden verschiedene Faktoren untersucht, welche die Implementierung von Cybersicherheit als Instrument des betrieblichen IT-Risikomanagements beeinflussen, und im Anschluss werden verschiedene Hypothesen über die Auswirkungen dieser Faktoren diskutiert (Bandyopadhyay T., 2012). Außerdem werden die Möglichkeiten der Integration von Cyber-Policen als wesentliche Komponente des IT-Risikomanagements untersucht und es wird erklärt wie spezifische Versicherungslösungen in den Risikomanagementkreislauf integriert werden können (Siegel, 2002). Dazu wurde ein umfassender Rahmen für die Einbeziehung von Cyber-Versicherungen in das Management von Informationssicherheitsrisiken anhand des gesamten Risikomanagementprozesses erstellt (Gordon, 2003). Außerdem wurden die wichtigsten Komponenten eines umfassenden Cyber-Risikomanagement unter Berücksichtigung relevanter Sicherheitsstandards untersucht und diskutiert (Kosub, 2015).

An der Cyber-Versicherung wurde kritisiert, dass sie von den Versicherungsunternehmen unklar formuliert wird (Eling M. W., 2016; Palsson, 2020). Der

derzeitige Markt für Cyber-Versicherungen ist fragmentiert. Versicherer bieten unterschiedliche Policen an, die verschiedene Arten von Cyberrisiken abdecken. Diese Fragmentierung macht es für Käufer schwierig, eine umfassende Deckung für Cyberrisiken zu erhalten (Dobias, 2022). Darüber hinaus weisen Cyberversicherungspolicen häufig niedrige Versicherungslimits und zahlreiche Ausschlüsse auf, was ihre Wirksamkeit bei der Minderung von Cyberrisiken einschränkt (Haitham, 2023). Es wird erwähnt, dass dieser Teilversicherungsmarkt noch zu klein ist und die Nachfrage hauptsächlich durch IT-abhängige Unternehmen induziert wird, sodass diese Sparte unattraktiv für Versicherer ist (Bandyopadhyay T. M., 2009). Die Informationsasymmetrie und die globalen, hochkorrelierten Schadenspotenziale von Cyberrisiken werden in der Literatur häufig als wichtige Marktbarrieren für das Angebot von Cyberpolicen genannt (ENISA, 2018; OECD, 2017). Zusätzlich haben die fehlenden Erfahrungen mit der Schadensregulierung, sowie die fehlende historische Datenbasis zu den Häufigkeiten und Risiken von Cyberbedrohungen, Auswirkungen auf den von Versicherungen durchzuführenden Prozess der Risikoanalyse und -beurteilung (Tøndel, 2015). Versicherer prognostizieren kundenseitige Folgeschäden und Reputationsverluste aus Cybersicherheitsvorfällen nur unzureichend. Die Folge ist, dass die Kosten für Cyberpolicen tendenziell zu hoch sind (Bandyopadhyay T., 2012). Verstärkend kommt hinzu, dass die Risikoanalyse, welche vor dem Versicherungsabschluss durch die Versicherung durchgeführt werden muss, hauptsächlich darauf abzielt, allgemeine Informationen zur IT-Sicherheit zu sammeln. Dabei werden Schutzmaßnahmen, die Unternehmen bereits ergriffen haben, nicht ausreichend berücksichtigt (Shetty, 2010). Außerdem wurde die inhaltliche und strukturelle Ausgestaltung der Antragsunterlagen für Cyber-Versicherungen untersucht, um Informationen zu den IT-Sicherheitsmaßnahmen der Unternehmen zu erheben und zu dokumentieren (Woods, 2017). Versicherer verwenden einen umfangreichen Fragenkatalog, führen Telefoninterviews und Kundenpräsentationen durch, und sammeln damit die notwendigen Informationen, um die IT-Sicherheitsmaßnahmen der Unternehmen zu bewerten (Woods, 2017). Außerdem werden verschiedene Methoden diskutiert, die Versicherer zur Bewältigung gezeichneter Cyberrisiken auf dem Erstversicherungsmarkt einsetzen können (Zhao, 2013; Eling M. W., 2016). Versicherer unterstützen dabei KMU durch Ihr Expertennetzwerk, bestehend aus Krisenberater, IT-Dienstleister, oder auch IT-Forensiker). Diese sind zwingend notwendig, da sich Cyberrisiken ständig weiterentwickeln und das in einem sehr schnellen Tempo (Kuhlee, 2023).

Forscher haben auf dem US-amerikanischen Versicherungsmarkt Cyber-Policen analysiert, um Erkenntnisse zum Underwriting-Prozess zu gewinnen und das Verständnis von Versicherungen für Cyberrisiken sowie deren Bepreisung zu gewinnen (Romanosky S. A., 2017). Außerdem hat die USA mehr Cyberschäden als Europa gemeldet (Gambacorta, 2022). Somit stellt sich die Frage, ob

hier ein anderes Meldeverfahren vorliegt, welches den Versicherungen und Versicherten helfen könnte, einen nachhaltigeren Cyber-Versicherungsmarkt zu schaffen.

Zusammenfassend hat sich gezeigt, dass es eine umfangreiche Literatur zum Thema Cyber-Versicherung und Einbindung in das Risikomanagement gibt. Jedoch gibt es wenig Literatur, welche sich auf den Bereich von KMU konzentriert. Aufgrund dieser bestehenden Forschungslücke konzentriert sich die vorliegende Arbeit auf den Cyber-Versicherungsmarkt im Bereich KMU und zeigt die Herausforderungen dieses Marktes. Ziel ist es, Gründe für die verhaltene Nachfrage an Cyberversicherungen bei KMU herauszuarbeiten, mögliche kritische Faktoren seitens der Versicherer aufzuzeigen und Lösungsstrategien zu deren Bewältigung zu entwickeln.

## 4. Methodik

Um die derzeitigen Herausforderungen für KMU im Markt von Cyberversicherungen zu ermitteln, werden Interviews mit Experten aus Beratungsgesellschaften, Versicherungs-unternehmen, Aufsichtsbehörden, Agenturen und Makler von Cyberpolicen geführt. Deren Einschätzungen bezüglich der Versicherbarkeit von Cyberrisiken bei KMU bilden u. a. die Grundlage dieser Studie. Sie ist quantitativ empirisch angelegt, damit ein möglichst differenziertes Verständnis der Markteinschätzungen seitens der Versicherungsunternehmen und KMU generiert wird. Diese Aspekte werden unter den gesetzlichen Rahmenbedingungen berücksichtigt. Da sowohl die Versicherbarkeit von Cyberrisiken bei KMU, als auch die Marktbarrieren neuartig sind, werden zur Beantwortung der Forschungsfrage qualitative Methoden der empirischen Sozialforschung verwendet. Ziel ist es durch die Auswertung des erhobenen praxisbasierten Handlungs- und Erfahrungswissen der befragten Experten neue Erkenntnisse zu gewinnen (Schnell, 2011). Die qualitative Forschungsmethode besitzt dabei den entscheidenden Vorteil neue Theorien und Hypothesen abzuleiten (Diekmann, 2007; Finfgeld-Connett, 2014). Einen Überblick über das ausgearbeitete Forschungsdesign ist in Abbildung 1 zu sehen. Auf Basis der Literaturrecherche erfolgt die Formulierung eines konzeptionellen Rahmens, welcher die Grundlage für die Untersuchung bildet (Cepeda, 2005; Yin, 2014), wichtige Aspekte der Versicherbarkeit von Cyberrisiken bei KMU identifiziert und Gründe für die geringe Versicherungsquote aufzeigt. Als Befragungsform wird die mündliche Befragung in Präsenz mittels teilstandardisierten Interviews gewählt, die sich insbesondere zur Ermittlung von Expertenwissen in der qualitativen Forschung etabliert haben (Hopf, 2013). Hierbei dienen die Experteninterviews als eine ermittelnde und informatorische Interviewform, um Wissensbestände zu erfahren (Lamnek, 2005). Die Durchführung eines Experteninterviews erfolgt mithilfe eines offenen Leitfadens (Myers, 2007; Kaiser, 2014), welcher alle relevanten

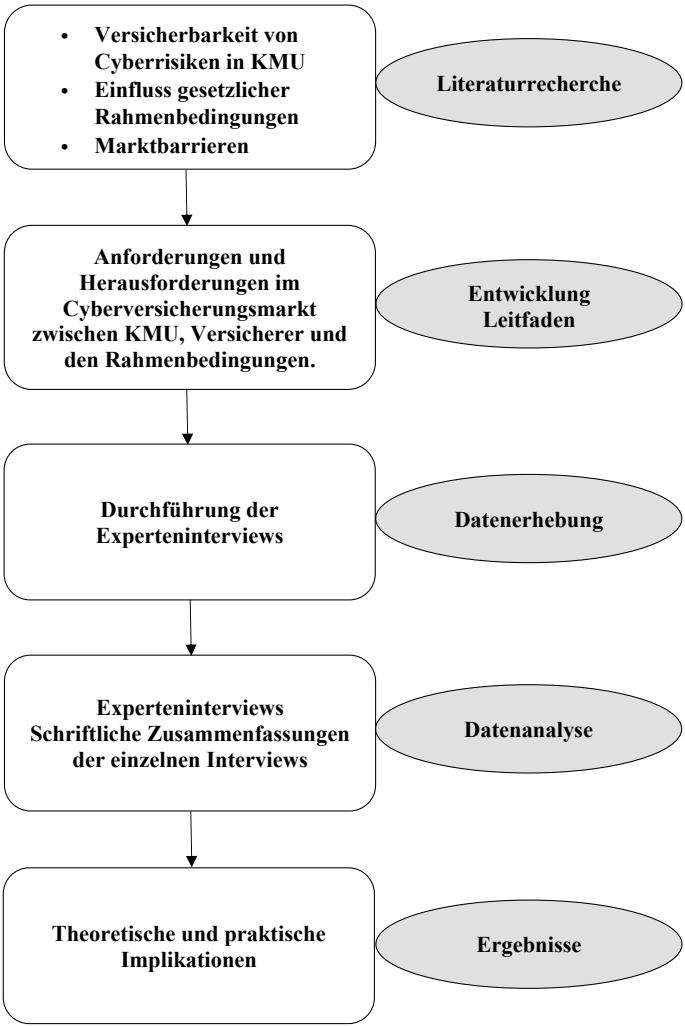


*Abb. 1: Bezugsrahmen und Elemente des Forschungsdesigns*

thematischen Problembereiche als eigenständig formuliertes Themenfeld beinhaltet (Modrow-Thiel, B., 1993). Auf die Durchführung eines Pretests konnte verzichtet werden, weil die Möglichkeiten der inhaltlichen Anpassungen und Ergänzungen des Interviewleitfadens nach Erhebung der ersten Interviews bestand (Gläser, 2010). Der Interviewleitfaden hat die nötige Detailtiefe, um auch weniger fundierte Themen eine angemessene Strukturierung für die Findung inhaltlich angemessener Antworten zu geben. Um den Einstieg in das Interview zu erleichtern dienen zu Beginn des Interviews allgemeine Fragen und Erläute-

rungen zum Forschungsvorhaben der Schaffung einer vertrauensvollen und angenehmen Gesprächsatmosphäre.

Die im Interview gestellten Fragen thematisieren die Cyberschäden in KMU, die Einbindung der Cyberpolice in das Cyber-Risikomanagement und die gesetzlichen Rahmenbedingungen. Die Fragen sind in die Bereiche „Risikomanagement", „Rahmenbedingungen" und „Cyber-Versicherung" eingeteilt. Dabei orientieren sich alle Fragen an den Ergebnissen der Literaturrecherche. Die abschließenden Fragen galten dem Optimierungsbedarf von aktuell vorhandenen Cyberpolicen und dem zukünftigen Trend bei Cyber-Versicherungen. Vor der Durchführung des Interviews wurden jedem Experten die Fragebögen zur Vorbereitung und frühzeitigen Klärung möglicher Fragen zur Verfügung gestellt. Die Experteninterviews wurden am Jahresende 2023 durchgeführt. Dabei fanden insgesamt 11 Interviews statt, in denen verschiedene Experten aus Beratungs- und Versicherungsunternehmen, Behörden und Vertrieb befragt wurden. Aufgrund der unterschiedlichen Bereiche wurden diese in Gruppen (A–C) eingeteilt (Tabelle 3).

Gruppe A umfasst Erstversicherungsunternehmen, die wichtige branchenspezifische Erkenntnisse zum Thema Cyberrisiken und Versicherungen bei KMU liefern. In der Gruppe B sind Beratungsgesellschaften und Behörden vertreten. Die hier – von außen betrachtet – gewonnenen Erkenntnisse ermöglichen somit eine objektive Einschätzung zum Marktgeschehen. In der Gruppe C werden aus Sicht von Versicherungsagenturen und Makler die aktuellen Mängel, oder die Probleme in der Umsetzung der Integration einer Cyber-Versicherung in das Cyber-Risikomanagement bei KMU aufgezeigt.

Aus diesen unterschiedlichen Blickwinkeln soll eine möglichst objektive und realistische Einschätzung des Marktes gewonnen werden. Die Auswahl der Befragungsteilnehmer erfolgte nicht nach Repräsentativitätskriterien, weshalb keine Zufallsstichprobe gezogen wurde. Die Auswahl der zu befragenden Experten orientiert sich im Wesentlichen an den Forschungsfragen (Bogner, 2014). Das umfassende Wissen des befragten Personenkreises über den gewählten Forschungsgegenstand lässt sich im Wesentlichen auf ein entsprechendes Betriebs- oder Kontextwissen zurückführen. Für die Informationsgewinnung der Marktbarrieren und Nachfrageforschungen für Cyber-Versicherungen im Bereich KMU, hat eine Befragung von 11 Experten stattgefunden. Dabei kamen 4 aus der Gruppe A (Versicherungsindustrie), weitere 4 aus der Gruppe B (Beratungsgesellschaften, Ratingagenturen, Behörden) und 3 aus der vertrieblich orientierten Gruppe C (Versicherungsagenturen/-makler). Die insgesamt 11 durchgeführten Interviews bieten somit eine stabile Ausgangsbasis für die qualitative Untersuchung und erlauben die Ableitung von Tendenzen und Entwicklungen (Hartley, 1994; Merkens, 1997; Marshall, 2013).

Die Befragung der Experten erfolgte in Präsenz oder telefonisch (Harvey, 1988; Sturges, 2004; Christmann, 2009; Cachia, 2011). Die Interviews wurden einzeln abgehalten, um die Wahrung der Vertraulichkeit der erhobenen Informationen sicherzustellen (Lamnek, 2005).

Aufgrund der sensiblen Daten und strengen Kontrollen wurde beim Interview kein Aufnahmegerät verwendet. Stattdessen wurde ein strukturiertes und systematisches Protokoll befolgt (Kin Cheah, 2019). Dieses Protokoll zielt darauf ab, die Genauigkeit und Transparenz der Interviews zu verbessern. Zusätzlich haben alle Interviewpartner eine Bestätigung unterschrieben, die Ihre Kontaktdaten und den Interviewablauf enthalten. Weiterhin haben die Interviewpartner den Fragebogen mit ihren abgegebenen Antworten zugeschickt bekommen, um diesen auf Echtheit der Informationen zu prüfen. Abschließend bestätigen sie die Angaben mit ihrer Unterschrift. Diese zusätzlichen Schritte erhöhen die Transparenz und untermauern die Echtheit der Ergebnisse. Allen Interviewpartnern wurde die Anonymität in Bezug auf Person und Firma in schriftlicher Form zugesichert.

*Tabelle 3*

**Teilnehmer der Expertenbefragung**

| Gruppe | Branche | Berufliche Position |
|---|---|---|
| A | Erstversicherer | Produktmanager und Underwriter Cyberversicherung |
| A | Erstversicherer | Underwriter |
| A | Erstversicherer | Abteilungsleiter IH Industrie Haftpflichtversicherung/Cyberversicherung |
| A | Erstversicherer | Leitung Cyberversicherung |
| B | Beratungsunternehmen | Geschäftsführer |
| B | Beratungsunternehmen | Geschäftsführer |
| B | Behörde | Referatsleiter |
| B | Ratingagentur | Managing-Analyst |
| C | Versicherungsagentur | Agenturleiter |
| C | Versicherungsagentur | Versicherungsfachwirt |
| C | Versicherungsmakler | Leiter Maklervertrieb |

## 5. Ergebnisse

Die nachfolgenden Abschnitte beschreiben die Ergebnisse aus den Experteninterviews. Die Ergebnisdarstellung erfolgt basierend auf den im Rahmen der Auswertung entwickelten Hauptkategorien.

### *5.1 Marktbarrieren*

In den Interviews wurde festgestellt, dass die Versicherungsunternehmen zur Erhebung der Risiken von KMU Fragebögen nutzen, welche gemeinsam mit dem einflussreichen Rückversicherer erarbeitet worden sind. Mit ihrer Hilfe wird die vorhandene IT-Infrastruktur des Unternehmens analysiert, um daraus die IT-Mindestanforderungen festzulegen. Die Fragestellungen fokussieren sich auf folgende Punkte, Back-Up, Firewalls, Virenscanner, Patchmanagement und Multifaktoridentifizierung. In der Praxis sind KMU mit der Bearbeitung der oft kompliziert aufgebauten Fragebögen teilweise überfordert, was leider zu falschen Angaben führt. Obwohl die Angaben von KMU von den Versicherungen nachträglich nicht verifiziert werden, erhalten sie dennoch eine Cyber-Versicherung. Hier besteht ein erheblicher Kritikpunkt, denn im Schadenfall drohen u. U. erhebliche Probleme bei der Schadenregulierung. Außerdem werden für Vertragsverlängerungen meist nur Umsatzzahlen und signifikante Veränderungen nachgefragt. Dieser Vorgang dient den Versicherungsunternehmen lediglich für die Einordnung des versicherten Unternehmens. Sollte das Unternehmen bestimmte Grenzen überschreiten, so zählt dieses beim Versicherer nicht mehr als KMU, sondern als größeres Unternehmen und wird mit höheren IT Anforderungen beauflagt. Ebenfalls wird bei der Abfrage kritisch betrachtet, dass das Cyber-Risiko ein dynamisches Risiko ist, was bedeutet, dass Schwachstellen und neue Risiken kontinuierlich neu erhoben und bewertet werden müssen. Weder Versicherungsunternehmen noch KMU besitzen hier die Kernkompetenz, was die Richtigkeit der Erhebung erschwert.

Ein weiterer Kritikpunkt ist die Deckungssumme einer Cyber-Versicherung. Die Versicherer sind der Auffassung, dass eine Mindestdeckung nicht sinnvoll ist, da der Fokus auf die zügige „Wiederinbetriebnahme" des Unternehmens liegen soll und eine Mindestdeckung hier einen falschen Anreiz setzten würde. Die Schäden sind momentan noch zu gering und KMU wissen selber nicht welcher finanzielle Schaden bei einem Hackerangriff im „worst case" Szenario droht. Aufgrund dessen können sie auch aus der Mindestdeckung keinen Nutzen ziehen. Aktuelle Schadensersatzansprüche aufgrund Verstöße gegen die DSGVO haben z. Z. nur eine geringe Erfolgswahrscheinlichkeit. Sollte sich jedoch diesbezüglich der Schadensanspruch in den nächsten Jahren erhöhen, sehen die Experten eine Mindestdeckung in der Haftpflicht als sinnvoll.

Auf dem Weg zu mehr Cybersicherheit ist es von größter Bedeutung, dass auch die Geschäftsführung für dieses Thema sensibilisiert wird. Dabei müssen Sie ihr Wissen auf diesem Gebiet kontinuierlich erweitern, denn sie geben auch im IT-Bereich die notwendige strategische Unternehmensausrichtung vor.

### *5.2 Standardisierung*

In den Interviews wurde deutlich, dass es derzeitig keine Standardisierung im Produkt oder in den Anforderungen einer Cyber-Versicherung gibt. Versicherungsunternehmen unterscheiden zwischen kleine und große Unternehmen, wobei Erstere lediglich ein Antragsformular nebst Fragebogen auszufüllen haben. Bei größeren Unternehmen wird eine Prüfung vor Ort mit externen Experten durchgeführt. Die Grenzen – ob großes, oder kleines Unternehmen – bestimmen die Versicherungen selbst, und diese sind sehr variabel. In den Interviews lag die Spanne für den Jahresumsatz zwischen 5 Millionen Euro bis 150 Millionen Euro. Auch die Fragebögen sind sehr unterschiedlich gestaltet, was Angebotsvergleiche deutlich erschwert. Aufgrund dieser Heterogenität heben die Interviewpartner besonders hervor, dass es umso wichtiger ist, die Angriffsvektoren genau zu kennen. Nur weil eine Versicherung bestimmte Sicherheitsmaßnahen nicht fordert, kann sie dennoch für das Unternehmen sinnvoll sein. Um eine Auflistung der Angriffsvektoren zu erhalten und gezielte Abwehrmaßnahmen einzuleiten bietet sich ein externer Check an. Aber auch das Versicherungsunternehmen profitiert durch einen einheitlichen Fragebogen, indem es z. B. bei bestimmten Anforderungen im Fragebogen weniger in Erklärungsnot gerät.

Geteilter Meinung sind die Experten, inwieweit für ein Cyber-Versicherungsangebot eine externe Beratungsgesellschaft den IT-Sicherheitscheck bei KMU durchführen muss. Die Versicherer (Gruppe A) sind der Auffassung, dass Sie diesen eigenständig durchführen können und ihre Verträge entsprechend den erarbeiteten Kriterien kalkulieren. Ein externes Beratungsunternehmen ist teuer und würde sich letztlich auf die Prämien auswirken. Die Experten der Gruppe B und C sind der Meinung, dass externe Beratungsunternehmen die Transparenz und die Standardisierung fördern. Außerdem fehlt es den Versicherungen oft an Know-how die Cyberrisiken von KMU zu bewerten, da es nicht zu ihrer Kernkompetenz gehört. Außerdem halten sie es für sinnvoll Cyberversicherungen transparent und für den Geschäftskunden einfach vergleichbar zu gestalten, was am Markt bei den Versicherungen für entsprechenden Preisdruck führen würde. Weitere Interviewpartner aus dieser Gruppe sind der Ansicht, dass es zweitrangig ist, ob der IT-Sicherheitsstand von externen Beratungsgesellschaften, oder von den Versicherungsunternehmen selbst erstellt wird, denn im Fokus muss die Standardisierung stehen. Fraglich ist, wie diese aussehen soll. Hier gibt es mehrere Ansätze wie die ISO oder der Risikomatrix.

Außerdem raten die Interviewpartner den Unternehmen ein strukturiertes Risikomodell anzuwenden, welches Softwareanbieter in ihren Produkten bereits integriert haben. Mithilfe dieser Risikomodelle können die Unternehmen Ihre Cybersicherheit erhöhen. Jedoch stehen den Versicherungen zur Bewertung der IT-Sicherheit diese detaillierten Daten aus Datenschutzgründen nicht zur Verfügung, was von den Interviewpartnern als großer Kritikpunkt angesehen wird. Abzuraten ist jedoch KMU einen obligatorischen Fragebogen ausfüllen zu lassen, welcher als Grundlage der Risikobewertung dient. Hier ist das Gap zwischen dem Anspruch und der Wirklichkeit zu groß.

### *5.3 Cybersicherheitsbewusstsein*

KMU müssen sich dem Individuellen Risiko bewusst werden. Dabei wird bei dem Bewusstsein zwischen dem Individuellen Risiko und dem Allgemeinen Risiko unterschieden. KMU ist das Allgemeine Risiko zwar bewusst allerdings nicht das Individuelle. Hier haben viele Unternehmen den Ansatz, dass deren Daten für Hackerangriffe nicht relevant sind, ihr Unternehmen zu klein ist und damit für Cyberkriminelle unbedeutend. Die Realität sieht allerdings anders aus, denn die Interviewpartner leisten wichtige Aufklärungsarbeit beispielsweise durch Lageberichte, Newsletter oder eigenen Studien. Allerdings verstärken diese Punkte nur das Allgemeine Risiko und nicht das Individuelle Risiko bei KMU. Letztgenanntes Risiko ist den Geschäftsführern nur bedingt bewusst und sie haben auch nicht das Know-how und die Zeit sich damit intensiv zu beschäftigen. Damit dieses Individuelle Risiko dem Geschäftsführer bewusst wird, wurde angeregt, dass der Vertrieb aktiver auf diese Geschäftskunden zugeht.

Grundsätzlich stellte sich in den Interviews heraus, dass die Versicherungsvermittler nicht aktiv die Kunden zugehen. Sie gehen davon aus, dass Wissensdefizite die Akquisition erschweren und gezielte Schulungsmaßnahmen notwendig sind. Passend dazu wurde im Interview mit den Erstversicherern die Vermutung geäußert, dass die mangelnde Schulungsteilnahme in der Altersstruktur des Vertriebes liegt und der Komplexität des Produktes. Diese sei kurz erklärt: Die Komplexität einer Cyber-Versicherung besteht aus der Kombination aus Haftpflicht, Sachversicherung und Betriebsunterbrechung. Die Übergänge sind hier schwebend. In den Gesprächen mit dem Vertrieb stellte sich heraus, dass sie zu viele Produkte im Sortiment haben und daher auf die einzelnen Nischenprodukte nicht genauer eingehen können, weshalb sie das Produkt als nicht wichtig genug ansehen.

Geht es um den Verantwortungsbereich der Cybersicherheit, so ist dieser klar definiert, es fehlt jedoch an der notwendigen Sensibilisierung. Die Geschäftsführer müssen – laut Aussage der Interviewpartner – die Dringlichkeit der Cy-

bersicherheit erkennen und sich mit der Thematik auseinandersetzten, denn oftmals wird die IT-Abteilung im Unternehmen nur als Kostenblock identifiziert und mit geringem Budget ausgestattet. Dabei werden Cyber-Versicherung und IT-Sicherheit von den Geschäftsführern teilweise als Substitute angesehen. Zudem haben IT-Mitarbeiter erfahren, dass es als Zeichen von schlechter Arbeit aufgefasst wird, wenn das Unternehmen eine Cyber-Versicherung kauft. Das ist ein eindeutiges Indiz für das fehlende Bewusstsein bei den betreffenden Geschäftsführern in Bezug auf die Abhängigkeit des Unternehmens von der IT und der exponierten Stellung der IT-Sicherheit im Unternehmen. Die Cyber-Versicherung ist nach Worten der Interviewpartner als Baustein der IT-Sicherheit anzusehen und dient zur Absicherung des Restrisikos und ist keinesfalls als Substitut der IT-Sicherheit zu betrachten. Leider haben das viele KMU noch nicht verinnerlicht. Um hier Vorsorge zu treffen, wird von den Interviewpartnern eine Vorsorgepflicht für die Cyber-Versicherung empfohlen. Diese IT-Sicherheit ist dann ständig zu kontrollieren und auch die IT-Rechte müssen klar abgegrenzt werden.

Zusammenfassend ist für die Unternehmen das Cyberrisiko insolvenzbedrohend. Daher ist das Ziel, die Cybersicherheit so in die Unternehmenskultur zu integrieren, dass sie auch von den Mitarbeitern bewusst gelebt wird. Laut Experteninterview ist das bislang noch nicht erreicht.

### *5.4 Rahmenbedingung*

Im Interview wurde erwähnt, dass es in Deutschland ein Meldeverfahren gibt, welches von KMU nur selten genutzt wird. Grund hierfür ist die Angst vor Reputationsschäden und der dafür erforderliche Zeitaufwand, denn die Meldung solcher Cyberangriffe ist sehr kompliziert. Der Meldeprozess selbst wurde ebenfalls kritisiert. Sie empfehlen ein „One-Stop-Formular", welches alle Interessentengruppen erreicht. Derzeitig werden zu viele Dokumente von unterschiedlichen Interessentengruppen benötigt, was einen erheblichen Bearbeitungsaufwand darstellt. Im Gegensatz dazu wurde im Interview das Meldeverfahren der USA genannt. Kommt es hier zu Cyberattacken mit Lösegeldforderungen ist dies vom Staat zu genehmigen. Hier waren die meisten Experten davon überzeugt, ein solches Meldeverfahren auch in Deutschland umzusetzen, um das Geschäftsmodell von Cyberkriminellen unattraktiver zu gestalten.

In den Interviews wurde klar, dass die neuen Richtlinie NIS 2.0 bei den Experten in der Kritik steht. Eine große Hürde ist die zeitliche Umsetzung. Damit ein Unternehmen die Richtlinien erfüllen kann, benötigt es Zeit, Ressourcen und Kosten. Diese Faktoren müssen unbedingt berücksichtigt werden. Außerdem bestehen Bedenken hinsichtlich der Bekanntheit und des Verständnisses der NIS 2.0.

Ein weiterer Punkt im Interview galt den Prämien einer Cyber-Versicherung. Diese schwanken sehr stark und sind in den vergangenen Jahren zwischen 300 – 400 % gestiegen. Auch neue Versicherer drängen in den Mark und werben mit Niedrigpreisen. Sie steigen nach ein paar Jahren aus dem Markt bzw. erhöhen die Beiträge drastisch, was für viel Unruhe sorgt. Eine Preisstabilität würde für KMU mehr Planungssicherheit bedeuten und einen nachhaltigen Cyber-Versicherungsmarkt ermöglichen.

### *5.5 Expertennetzwerk*

Der größte Nutzen einer Versicherungspolice für KMU ist das Know-how und Expertennetzwerk des Versicherers. Dieses besteht beispielsweise aus IT-Forensiker, IT-Experten, Anwälte, PR-Berater, oder IT-Krisenmanager. Bei einem Angriff hat das versicherte Unternehmen sofortigen Zugriff auf dieses Netzwerk, welches am Markt kaum oder nur mit sehr hohen Kosten zu bekommen ist.

In den Interviews geraten die IT-Forensiker häufig in die Kritik. Aktuell gibt es nur wenige IT-Forensiker am Markt, weshalb alle größeren Versicherer folglich auf die Gleichen zugreifen. Diese meinen zwar im Falle eines Kumulschadens allen Betroffenen die benötigte Hilfe zukommen zu lassen, einen realen Test gibt es aber nicht. Die Interviewpartner gehen hier von einer Überlastung der IT-Forensiker aus, was mit dementsprechenden Bearbeitungsverzögerungen einhergeht. Außerdem mangelt es hier an Transparenz bei den spezifischen Qualifikationen der IT-Forensiker, da derzeitig noch keine Zertifikate definiert wurden. In den Versicherungsverträgen sind IT-Forensiker folglich anonymisiert und im Schadensfall weiß der Kunde nicht, welcher fachspezifische IT-Forensiker zu Hilfe kommt.

### *5.6 Cyber-Versicherungsmarkt und zukünftige Potenziale der Cyber-Versicherung*

Die Experten gehen in den nächsten Jahren von einer verstärkten Nachfrage von Cyber-Versicherungen aus. Grund dafür sei die weiter steigende Abhängigkeit vom Internet und die daraus entstehenden Risiken. Derzeitig haben die Versicherer und Beratungsunternehmen Bedenken in Bezug auf die Tragfähigkeit für die Versicherungsunternehmen. Es wird geäußert, dass der Bestand in den Büchern zu klein ist, um ein Ausgleich im Kollektiv zu gewährleisten. Das Cyberrisiko ist ein Kumulrisiko, was hohe Schadensummen verursachen kann. Wird z. B. ein großer Cloudanbieter gehackt, so hat nicht nur dieser einen großen Schaden, sondern u. U. auch viele daran angeschlossene Unternehmen, da die Sicherheitslücke des Cloudanbieters von den Cyberkriminellen als Einfalls-

tor bei fremden Unternehmen genutzt werden kann. Die Anhängigkeiten sind hier also enorm.

Für die Versicherungsunternehmen werden Start-ups, die sich mit IT-Sicherheit beschäftigen, immer interessanter. Diese Branche ist sehr schnelllebig und da Versicherungsunternehmen immer bestrebt sind auf dem aktuellsten Stand zu sein, ermöglichen Start-ups eine kostengünstige Erweiterung ihres Netzwerks.

Derzeitig stehen noch keine konkreten Begriffe wie „IT-Schäden" in den Verträgen. Deshalb müssen die Verträge konkreter formuliert werden, denn beide Vertragspartner müssen wissen, welche Schäden wie abgedeckt werden. Es werden hier Musterbedingungen gefordert.

## 6. Diskussion

Die Ergebnisse dieser Studie zeigen, dass der Cyber-Versicherungsmarkt für KMU im Wandel ist. Sie verdeutlicht, die mangelnde Auseinandersetzung KMU mit der eigenen Risikolage und der damit verbundenen nicht ausreichenden IT-Sicherheit. KMU ist häufig nicht bewusst, wie abhängig sie von ihrer IT sind und wie essenziell hierfür die Sicherheitsmaßnahmen sind. Geschäftsführer und Mitarbeiter müssen sensibilisiert werden, um das Individuelle Risiko zu erkennen. Als sinnvoll wird hier ein sogenannter „Cyber-Führerschein" von den Experten erachtet, welcher von Versicherungen, oder auch von staatlichen Institutionen angeboten werden sollte. So erkennen die Geschäftsführer die Gefahr und können Aufgaben an IT-affinere Mitarbeiter auslagern. Als Möglichkeiten für die Sensibilisierung werden in den Interviews kontinuierliche Schulungen erwähnt.

Die Versicherungsunternehmen müssen mehr auf das individuelle Risiko von KMU eingehen. Derzeit gibt es viele Studien und Berichte, welches zur Sensibilisierung des Allgemeinen Risikos beiträgt, jedoch nicht zum Individuellen Risiko. Der Vertrieb benötigt mehr Spezialisierung und das schon in der Ausbildung. Außerdem gebe es zu wenig Schulungsangebote und Sensibilisierungsmaßnahmen für die Mitarbeiter der Versicherungen. Hier müssen Pflichtschulungen und vermehrte Sensibilisierungsmaßnahmen angeboten werden. Ein großes Problem derzeitig ist das mangelnde Fachpersonal. Aufgrund der Produktvielfalt ist es realistisch, dass es in Zukunft Vertriebsspezialisten ausschließlich für Cyber-Versicherungen gibt. Zwangssensibilisierung durch Richtlinien, wie die NIS 2.0 helfen derzeitig nur bedingt. Hier muss besonders KMU bei der Umsetzung der NIS 2.0 geholfen werden. Ein weiterer Kritikpunk: Länderübergreifend agierende Unternehmen müssen unterschiedliche Sicherheitsstandards vorweisen, da es keine einheitlichen Richtlinien EU-weit gibt. Positiv ist allerdings, dass die NIS 2.0 für mehr Kommunikation in den Unternehmen

bezüglich der IT-Sicherheit sorgt, da beispielsweise im Zuge der Lieferkettensituation die größeren Unternehmen sich nach den Sicherheitsstandards von KMU erkundigen müssen. Sollten diese dann nicht den Mindestanforderungen gemäß NIS 2.0 genügen, ist eine weitere Zusammenarbeit nicht gesetzeskonform. Auch ist der Notfallplan, welcher in vielen Unternehmen existiert, als äußerst positiv zu bewerten. Dieser sollte jedoch nicht nur in den von der Richtlinie NIS 2.0 betroffenen Unternehmen gelten, sondern für alle Unternehmen. Ebenfalls die darin enthaltene Schulungspflicht ist sehr positiv zu bewerten. Allgemein ist festzuhalten, dass die NIS 2.0 einen guten Einblick in die IT-Sicherheit gibt und als Ansatz für eine Zwangssensibilisierung dient. KMU haben jedoch wenig Know-how und die mangelnde Bekanntheit der NIS 2.0 macht es derzeitig schwierig die Richtlinie umzusetzen.

Die Studie zeigt auch die derzeitig mangelnde Standardisierung bei der Erhebung des Risikos durch Fragebögen, welche unverständliche formuliert sind. In der Praxis beantworten KMU den Fragebogen häufig fehlerhaft – aus Unwissenheit oder auch bewusst, nur um eine Cyber-Versicherung zu bekommen. Letzteres hätte ggfs. den Verlust des Versicherungsschutzes zur Folge. Hier müssen Versicherer mehr Kontrollen einlegen und die Fragebögen im Nachgang verifizieren. Des Weiteren müssen die Fragebögen deutlicher, klarer und greifbarer für den Kunden ausgestaltet werden. Hier würden anhängende Beispiele, oder zusätzliche Erklärungen für mehr Klarheit sorgen.

Außerdem sind die Grenzen, bis wann ein Unternehmen als KMU zählt, aktuell zu heterogen. Ein neues Konzept für die Risikoerhebung wird befürwortet, da der Unterschied zwischen den Anforderungen in den Fragebögen und der Umsetzung in der Realität zu groß ist. Durch die Komplexität des Produktes sind auch die von der Versicherung angebotenen Dienstleistungen, sehr unterschiedlich. Diese Tatsachen führen dazu, dass ein bestimmtes Know-how und ein erheblicher Zeitaufwand von KMU benötigt werden, um die Produkte miteinander vergleichen zu können. Andernfalls ist ein Vergleich kaum möglich.

Das Meldeverfahren in Deutschland steht sehr in der Kritik. Die meisten Experten waren der Meinung, dass ein Meldeverfahren – ähnlich dem der USA – deutlich attraktiver wäre. Zu klären wären hier die zu ziehenden Grenzen z. B. ab wann in Abhängigkeit zur Schadenshöhe ein Cyberangriff gemeldet werden muss, um u. a. auch professionelle Hackerbanden abzuschrecken. Das Gegenargument der hohen Kosten für das Unternehmen beim Aufbau einer eigenen Cyberabwehr wurde im Interview entkräftet. Die Experten sind diesbezüglich der Auffassung, dass nach einem Hackerangriff jedes Unternehmen die gesamte IT erneuern muss, um wieder ein geeignetes Sicherheitsniveau zu haben und das ist mit sehr hohen Kosten verbunden. Wird das Sicherheitsniveau nicht wiederhergestellt, haben die Hacker leichtes Spiel erneut in das Unternehmen einzudringen. Im Falle eines Cyberangriffs muss das Unternehmen davon ausgehen,

dass die gestohlenen Daten – auch im Falle einer Lösegeldzahlung – von den Cyberkriminellen nie gelöscht werden, sondern an die Konkurrenz verkauft, oder später veröffentlicht werden. Diese These unterstützt das Argument, dass ein Unternehmen sich nach einem Hackerangriff IT-spezifisch neu aufbauen muss und befürwortet das Meldeverfahren der USA.

Der größte Nutzen des Versicherers liegt im Experten-Netzwerk. KMU haben im Schadenfall enorme Vorteile, wenn sie auf das Expertennetzwerk der Versicherungen zugreifen können, um den Schaden zu beheben. Allerdings fehlt es hier an Transparenz. IT-Forensiker stehen in der Kritik keine Qualitätsmerkmale in Form von Zertifikaten aufweisen zu müssen. Auch wird in den Versicherungsverträgen kein IT-Forensiker explizit genannt, was ebenfalls zu mangelnder Transparenz führt. Hilfreich wären hier gut strukturierte Zertifikate, um die Stärken/Qualifikationen der jeweiligen Spezialisten zu erkennen – eine Maßnahme, die im Markt für mehr Transparenz sorgen würde.

Da Cyberrisiken sowohl innerhalb von Unternehmen als auch betriebsübergreifend oft stark voneinander abhängig sind, besteht eine erhöhte Wahrscheinlichkeit, dass im Rahmen einzelner Cybervorfälle schwerwiegende kumulierte Schäden auftreten können. Dies kann zu einer bedeutenden Kumulschadenproblematik führen. KMU berücksichtigen leider nicht ausreichend die enormen Auswirkungen von Cyberangriffen auf die Liefer- und Wertschöpfungsketten zwischen den Unternehmen und haben dazu kaum effektive Risikovermeidungs- und -bewältigungsstrategien. In Zusammenarbeit mit den Versicherungsunternehmen muss daher ein innovatives Deckungskonzept für solche Risiken entwickelt werden. Die Experten sind der Ansicht, dass spezifische Kumule gebildet werden müssen, damit sich die Tragfähigkeit der Versicherer erhöht. Um einen finanziellen Kollaps der Branche bei einem Kumulschaden zu vermeiden, wurde der Ansatz geäußert, den Staat finanziell mit in die Verantwortung zu nehmen. Hier müssten allerdings Richtlinien entworfen werden, welche der Unternehmen unter diesen Schutzschirm gehören. Ein denkbarer Ansatz wäre z. B. alle, für das Land „systemrelevanten Unternehmen", aufzufangen.

Wie die meisten qualitativen Studien weist auch die vorliegende Untersuchung Limitationen auf, die hauptsächlich in den Besonderheiten des qualitativ-methodischen Vorgehens begründet sind. Die kleine Stichprobe der befragten Unternehmen ist nicht ausreichend, um die Repräsentativität zu gewährleisten. Die Verallgemeinerung der Erkenntnisse ist begrenzt, da abhängig vom strategischen Management der Versicherer die Bedeutung einer Cyber-Versicherung unterschiedlich ausfallen kann. Das wiederum hätte Auswirkungen auf den Fokus der Versicherungsprodukte und den damit verbundenen Maßnahmen hätte. Dies gilt ebenso für die gewonnenen Erkenntnisse über die zukünftige Entwicklung der Cyber-Versicherung, da einerseits Zukunftsprognosen grundsätzlich mit Unsicherheit behaftet sind und andererseits länderspezifische Besonderhei-

ten für die einzelnen Versicherungsmärkte stets eine wichtige Rolle spielen. Weiterführend wird in der Studie eine Verallgemeinerung von KMU vorgenommen. Je nach Branche und Ausrichtung des Risikomanagements, sind hier unterschiedliche IT-Sicherheitsmaßnahmen und Sensibilitäten der Geschäftsführer und Mitarbeiter zu nennen, welche im Gegensatz zur Studie auch zu anderen Ergebnissen führen kann. Eine weitere Einschränkung in Bezug auf die Aussagekraft der Erkenntnisse dieser Untersuchung ergibt sich aus der Einschätzung der Bedeutung von Cyber-Versicherungen durch die befragten Personen. Als externe Branchenexperten beurteilen sie die Bedeutung von Cyber-Policen und IT-Sicherheitsmaßnahmen für KMU aufgrund ihrer beruflichen Erfahrung. Diese Beurteilungen weisen eine gewisse Subjektivität auf und können vor dem Hintergrund des begrenzten Wissensstandes über die Gestaltung der unternehmensindividuellen Risikomanagementkonzepte beeinflusst werden und somit u. U. zu einer Überversicherung von Cyberpolicen bei KMU führen. Forschungsbedarf liegt derzeitig bei Standardisierungsmodellen von Cyber-Versicherungen sowie innovativen Deckungskonzepten vor.

## 7. Zusammenfassung und Schlussbemerkung

Dieser Artikel befasst sich mit zentralen Fragen der zurückhaltenden Nachfrage an Cyber-Versicherungen bei KMU. Für Unternehmen, unabhängig von ihrer Branche und Größe, ist die Bedrohung durch Cyberattacken real und sollte, wie alle Unternehmensrisiken, umfassend analysiert werden. Mithilfe von branchenspezifischen Experteninterviews wurden anhand von qualitativen Fragebögen Ergebnisse gewonnen, um so die eingehende Forschungsfrage – „Warum ist der Cyber-Versicherungsmarkt, trotz erheblicher Relevanz bei KMU sehr verhalten?“ – zu beantworten. Es folgen zu den Ergebnissen ebenfalls auch die Lösungsansätze.

So fehlt es zum einen den KMU und Vertrieblern an Sensibilität. Das Gap zwischen dem Allgemeinen und Individuellen Risiko ist erheblich. Versicherungsunternehmen und Behörden erarbeiten Statistiken und betreiben Forschungen, welches in der Praxis als Aufklärung des Allgemeinen Risikos verstanden wird. Um ein Cyber-Risikobewusstsein bei den Geschäftsführern von KMU zu erzeugen, muss aktiv von den Versicherungsunternehmen auf diese zugegangen werden, mit dem Ziel sie zum Handeln zu bringen. Um das zu erreichen ist es zwingend notwendig im Vorfeld den Vertrieb zu sensibilisieren und intensiv zu schulen, was durch ergänzende Anreize seitens der Geschäftsführung unterstützt werden kann.

Zum anderen fehlt es immer noch an Standardisierungsansätzen. Fragebögen, welche bei KMU als Erhebung des Risikos dienen, sind von Versicherungsunternehmen zu heterogen. Die Fragen sind unklar und abstrakt formuliert, was

einige KMU überfordert. Folglich beantworten sie die Fragebögen nicht korrekt, was zu einer Verzerrung des tatsächlichen Risikos führt und die Erhebungsmethode deutlich in Frage stellt. Auch wird in den Versicherungspolicen das Netzwerk eines Versicherungsunternehmens nicht explizit erwähnt, was zu einer mangelnden Transparenz und schlechter Vergleichbarkeit beiträgt. Ein weiterer Punkt bei der Intransparenz sind die unterschiedlichen Grenzen der Versicherungsunternehmen. Es ist nicht einheitlich geregelt, ab wann ein Unternehmen einen Fragebogen ausfüllen muss und ab wann ein IT-Check mit externen Beratern erforderlich ist. Die Dienstleistungen einer Cyber-Versicherung sind an manchen Stellen undeutlich formuliert und müssen in Zukunft konkreter definiert werden. Um eine nachhaltige Cyber-Versicherung in einem zukunftsfähigen Cyber-Versicherungsmarkt anbieten zu können, müssen Standardisierungsmodelle entwickelt werden. Ansätze hierfür ist die Beauftragung externer Beratungsunternehmen, die z. B. einen größtenteils einheitlichen Fragebogen mit ggfs. kleinen branchenspezifischen Änderungen entwickeln. Auch würden sie den anschließenden IT-Sicherheitscheck bei KMU durchführen. Mit dem Ergebnis haben KMU die Möglichkeit Versicherungsangebote einzuholen, die auch einfach vergleichbar sind.

Cyber-Versicherungen stellen in der Versicherungswelt ein vergleichsweises neues Produkt dar. Der Markt ist demnach sehr volatil und die Anforderungen für Versicherer und KMU sind extrem elastisch. Damit dieser Markt nachhaltige Zukunftsaussichten hat, ist es essenziell ein innovatives Deckungskonzept zu entwickeln. Cyberrisiken haben eine hohe Ansteckungsgefahr. Dieses Kumulrisiko muss in Zukunft tragbar sein und abgeschwächt werden. Hier wird empfohlen Kumule zu bilden und Staaten als Rückversicherer einzubinden.

Diese Forschung hat einen Beitrag geleistet, welche die verhaltende Nachfrage nach einer Cyber-Versicherung bei KMU erklärt. Der größte Handlungsbedarf bei KMU besteht im erheblichen Gap zwischen dem Individuellen- und Allgemeinen Risiko. Um dieses zu reduzieren, sind weitere Untersuchungen empfehlenswert. Ergänzende Forschungsansätze für die Versicherer befinden sich z. B. im Bereich von alternativen Erhebungsmethoden für KMU, den Einflussmöglichkeiten der Rückversicherer auf den Cyber-Versicherungsmarkt oder auch den Möglichkeiten der Sensibilisierung des Vertriebs.

## Literaturverzeichnis

*Abhilash*, J. V. (2023): A Roadmap for SMEs to Adopt an AI Based Cyber Threat Intelligence. The Effect of Information Technology on Business and Marketing Intelligence Systems Studies in Computational Intelligence, S. 1903 – 1926.

*Anderson*, R. (1994): Liability and computer security: nine principles. (D. Gollmann, Hrsg.) Berlin: Springer.

*Böhme*, R. K. (2006): On the limits of cyber-insurance. (S. Fischer-Hübner, S. Furnell, C. Lambrinoudakis, Hrsg.). Springer.

BAFA (2012): Bundesamt für Wirtschaft und Ausfuhrkontrolle. Abgerufen im Januar 2024 von https://www.bafa.de/SharedDocs/Downloads/DE/Energie/ea_leitfaden_definition_kmu.html.

BaFin (25.5.2020): Bundesanstalt für Finanzdienstleistungsaufsicht. Abgerufen im Januar 2024 von https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/BaFinPerspektiven/2020/bp_20_1_Lohmann_Schmitz_Huy_Schulze_Wegerhoff.html.

*Bandyopadhyay*, T. (2012): AISeL. Abgerufen im Januar 2024 von https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1004&context=sais2012.

*Bandyopadhyay*, T. M. (2009): Why IT managers don't go for cyber-insurance products. ACM, 52(11), S. 706 – 719.

*Bauer*, J. V. (2009): Cybersecurity: stakeholder incentives, externalities, and policy options. Telecomm. Policy, 33(10 – 11), S. 706 – 719.

*Becker*, W. S. (2008): Deloitte Mittelstandsinstitut. Abgerufen im Januar 2024 von https://fis.uni-bamberg.de/server/api/core/bitstreams/ca7d0daa-4783-43c7-bd40-a6aafb80056e/content.

*Behringer*, S. (2012): Unternehmensbewertung der Mittel- und Kleinbetriebe Betriebswirtschaftliche Verfahrensweisen (Bd. 5). Hamburg: Erich Schmidt Verlag.

*Biener*, C. E. (2015): Cyber Risk: Risikomanagement und Versicherbarkeit. I VW HSG Schriftenreihe, 54.

*Blind*, K. (1996): Eine Analyse der Versicherung von Risiken der Informationssicherheit in Kommunikationsnetzen. Z. Ges. Versicherungswiss., 85(1), S. 81 – 101.

*Bogner*, A. L. (2014): Interviews mit Experten: Eine praxisorientierte Einführung. Wiesbaden: Springer VS.

*Bonn*, I. (2003): Institut für Mittelstandsforschung. Abgerufen im Januar 2024 von https://www.ifm-bonn.org/definitionen/kmu-definition-der-eu-kommission.

*Brancheau*, J. J. (1996): Key issues in information systems management. SIM Delphi results, 20(2), S. 225 – 242.

BSI (27.12.2022): NIS-2-Richtlinie im Amtsblatt der EU veröffentlicht. Abgerufen im Januar 2024 von Bundesamt für Sicherheit in der Informationstechnik: https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/KRITIS-aktuell/KRITIS-Meldungen/221227-veroeffentlichung-nis-2.html.

*Cachia*, M. M. (2011): The telephone medium and semi-structured interviews: a complementary fit. Qual. Res. Organ. Manage. Int. J., 6(3), S. 265 – 277.

*Cavusoglu*, H. C. (27.7.2004): Economics of ITSecurity Management: Four Improvements to Current Security Practices. Communications of the Association for Information Systems, 14, S. 65 – 75.

*Cebula*, J. P. (Mai 2014): A Taxonomy of Operational Cyber Security Risks Version 2. Abgerufen im Januar 2024 von Software Engineering Institute: https://insights.sei.cmu.edu/documents/2273/2014_004_001_91026.pdf.

*Cepeda*, G. M. (2005): A review of case studies. Management Decision, 43(6), S. 851 – 876.

*Chen*, Y.-C. L.-Y. (2022): The Effect of Cyber Risk Management Services in Insurance Policies. (D. M.-T. Dr. Cheng-Few Lee, Hrsg.) Emerald Publishing Limited.

*Choudhry*, U. (2014): Der Cyber-Versicherungsmarkt in Deutschland. Wiesbaden: Springer Gabler.

*Christmann*, G. (2009): Expert interviews on the telephone: a difficult undertaking. In: A. L. Bogner, Experts (S. 157 – 183). London: Palgrave Macmillan.

Destatis (2024): Statistisches Bundesamt. Abgerufen im Januar 2024 von https://www.destatis.de/DE/Themen/Branchen-Unternehmen/Unternehmen/Kleine-Unternehmen-Mittlere-Unternehmen/Glossar/kmu.html.

*Diekmann*, A. (2007): Empirische Sozialforschung: Grundlagen, Methoden, Anwendungen. Reinbek: Rowohlt.

*Dobias*, P. (2022): Insurance of Cyber Risk in International Transport. Masaryk University Journal of law and technology, 16(1), S. 3 – 36.

*Dyah*, H. D. (27.3.2023): Strategi Pengembangan Dan Pengelolaan UMKM Desa Kalikidang Banyumas Jawa Tengah. Jurnal Pengabdian Masyarakat Darul Ulum.

*Eling*, M. S. (November 2016): Ten Key Questions on Cyber Risk and Cyber Risk Insurance. The Geneva Association. Abgerufen im Januar 2024 von https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public//cyber-risk-10_key_questions.pdf.

*Eling*, M. W. (2016): Cyber Risk: Too Big to Insure? – Risk Transfer Options for a Mercurial Risk Class. Business, Law, Computer Science.

ENISA (2018): European Union Agency for Network and Information Security. Abgerufen im Januar 2024 von https://www.enisa.europa.eu/publications/incentives-and-barriers-of-the-cyber-insurance-market-in-europe/at_download/fullReport.

EP (10.11.2022): Europäisches Parlament. Abgerufen im Januar 2024 von https://www.europarl.europa.eu/news/de/press-room/20221107IPR49608/cybersicherheit-plane-zur-starkung-der-eu-weiten-widerstandsfahigkeit.

*Faisst*, U. P. (2007): Ein Modell zur dynamischen Investitionsrechnung von IT-Sicherheitsmaßnahmen. Z. Betriebswirtsch., 77(5), S. 511 – 538.

*Finfgeld-Connett*, D. (2014): Use of content analysis to conduct knowledge-building and theory-generating qualitative systematic reviews. Qual. Res., 14(3), S. 341 – 352.

*Gambacorta*, L. (2.6.2022): The drivers of cyber risk. Journal of Financial Stability.

GDV (19.4.2020): Gesamtverband der Versicherer. Abgerufen im Januar 2024 von https://www.gdv.de/gdv/themen/digitalisierung/vier-von-zehn-deutschen-schon-von-cyberattacken-betroffen-58642.

*Gläser*, J. L. (2010): Experteninterviews und qualitative Inhaltsanalyse als Instrumente rekonstruierender Untersuchungen. Wiesbaden: Springer VS.

*Gordon*, L. L. (2003): A framework for using insurance for cyber-risk management. ACM, 46(3), S. 81 – 85.

*Grzebiela*, T. (2002): Internet-Risiken: Versicherbarkeit und Alternativer Risikotransfer. Wiesbaden: Deutscher Universitäts-Verlag.

*Haas*, A. H. (2014): Risiken aus der Nutzung von Cloud-Computing-Diensten: Fragen des Risikomanagements und Aspekte der Versicherbarkeit. Zeitschrift für die gesamte Versicherungswissenschaft, 103(4), S. 377 – 407.

*Haitham*, N. A. (16.6.2023): Mapping cyber insurance: a taxonomical study using bibliometric visualization and systematic analysis. Global knowledge, memory and communication.

*Hartley*, J. (1994): Case studies in organizational research. In: Cassell, C., Symon, G. (Hrsg.) Qualitative Methods in Organizational Research: A Practical Guide (S. 209 – 229). London: SAGE.

*Harvey*, C. (1988): Telephone survey techniques. Can. Home Econ. J., 38(1), S. 30 – 35.

*Hiller*, J. R. (1.6.2013): The challenge and imperative of private sector cybersecurity: an international comparison. Computer Law and Security Review, 29(3), S. 236 – 245.

*Hopf*, C. (2013): Qualitative Interviews – Ein Überblick. In: U. V. Flick, Qualitative Forschung: Ein Handbuch. Reinbek: Rowohlt.

*Hoppe*, F. G. (19.11.2021): Cyber risk management in SMEs: insights from industry surveys. The Journal of Risk Finance, S. 240 – 260.

*Königs*, H.-P. (2017): IT-Risikomanagement mit System Praxisorientiertes Management von Informationssicherheits-, IT- und Cyber-Risiken (Bd. 5). Wiesbaden: Springer Vieweg.

*Kaiser*, R. (2014): Qualitative Experteninterviews: Konzeptionelle Grundlagen und praktische Durchführung. Wiesbaden: Springer VS.

*Kankanhalli*, A. T.-H.-K. (2003): An integrative study of information systems security effectiveness. Int. J. Inf. Manage., 23(2), S. 139 – 154.

*Katkova*, T. G. (2020): Provision of Cybersecurity in Ukraine. In: M. Nechyporuk/P. Vladimir/D. Kritskiy, Integrated Computer Technologies in Mechanical Engineering (S. 243 – 254). Springer.

*Kin Cheah*, P. P. (2019): Interviewing Criminal Justice Populations without Electronic Recording Devices: A Guide. The Qualitative Report, 24(4), S. 705 – 716.

*Kosub*, T. (2015): Components and challenges of integrated cyber risk management. Z. Ges. Versicherungswiss., 104(5), S. 615 – 634.

*Kuhlee*, L. (13.4.2023): pwc. Abgerufen im Januar 2024 von https://www.pwc.de/de/cyber-security/global-threat-intelligence-report.html.

*Lamnek*, S. (2005): Qualitative Sozialforschung. Basel: Beltz.

*Lebek*, B. U. (2014): Information security awareness and behavior: a theory-based literature review. Manage. Res. Rev., 37(12), S. 1049 – 1092.

*Lesch*, T. R. (2000): Risiken aus kommerzieller Nutzung des Internet – Möglichkeiten der Schadenverhütung und Versicherung. Z. Ges. Versicherungswiss, 89(4), S. 605 – 633.

*Luftman*, J. B.-Z. (2010): Key issues for IT executives 2009: difficult economy's impact on IT. MIS Q. Exec, 9(1), S. 49 – 59.

*Marshall*, B. C. (2013): Does sample size matter in qualitative research?: A review of qualitative interviews in is research. J. Comput. Inf. Syst., 54(1), S. 11 – 22.

*Meland*, P. T. (2017): Facing uncertainty in cyber insurance policies. (G. M. Livraga, Hrsg.) Springer.

*Merkens*, H. (1997): Stichproben bei qualitativen Studien. In: B. P. Friebertshäuser, Handbuch Qualitative Forschungsmethoden in der Erziehungswissenschaft (S. 97 – 106). München: Juventa.

*Modrow-Thiel*, B. (1993): Qualitative Interviews – Vorgehen und Probleme. Z. Personalforsch., S. 129 – 146.

*Mukhopadhyay*, A. C. (2013): Cyber-risk decision models: to insure IT or not? Decision Support Systems.

*Myers*, M. N. (2007): The qualitative interview in IS research: examining the craft. Inf. Organ., 17(1), S. 2 – 26.

*Njegomir*, V. M. (2012): Contemporary trend in the global insurance industry. Procedia Soc. Behav. Sci., 44, S. 134 – 142.

OECD (2017): Organisation for Economic Co-operation and Development. Abgerufen im Januar 2024 von https://www.oecd.org/daf/fin/insurance/Enhancing-the-Role-of-Insurance-in-Cyber-Risk-Management.pdf.

*Oğüt*, H. R. (2011): Cyber security risk management: public policy implications of correlated risk, imperfect ability to prove loss, and observability of self-protection. Risk Anal. 31(3), S. 497 – 512.

*Palsson*, K. G. (4.6.2020): Analysis of the impact of cyber events for cyber insurance. The Geneva Papers on Risk and Insurance – Issues and Practice, 45, S. 564 – 579.

*Petermann*, J. (19.7.2021): DW. Abgerufen im Januar 2024 von https://www.dw.com/de/experten-bedrohung-durch-cyberangriffe-steigt/a-58314785.

*Pfeiffer*, U. (17.12.2021): Eine starke Unternehmenskultur minimiert Cyberrisiken. Digitale Welt, 6(1), S. 24 – 27.

*Ransbotham*, S. M. (2009): Choice and chance: a conceptual model of paths to information security compromise. Inf. Syst. Res., 20(1), S. 121 – 139.

*Romanosky*, S. A. (2017): Content Analysis of Cyber Insurance Policies: How do Carriers Price Cyber Risk? Proceedings of the Southern Association for Information Systems Conference, Atlanta, (S. 23 – 29). USA.

*Romanosky*, S. S. (26.5.2023): Enterprise risk management: how do firms integrate cyber risk? Enterprise risk management.

*Ruan*, K. (2017): Introducing cybernomics: a unifying economic framework for measuring cyber risk. Computers & Security, 65, S. 77 – 89.

*Schnell*, R. H. (2011): Methoden der empirischen Sozialforschung. München: Oldenbourg.

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

*Shetty*, N. S. (2010): Competitive cyber-insurance and Internet security. In: T. P. Moore, Economics of Information Security and Privacy (S. 229 – 247). Boston: Springer.

*Siegel*, C. S. (2002): Cyber-risk management: technical and insurance controls for enterprise-level security. Inf. Syst. Secur., 11(5), S. 33 – 49.

*Smith*, G. (2004): Recognizing and preparing loss estimates from cyber-attacks. Information Systems Security, 12(6), S. 45 – 57.

*Soyer*, B. N. (2023): Cyber Risk Insurance – An Effective Risk Management Tool for SMES in the UK?. Edinburgh Law Review, 27(2), S. 157 – 184.

*Sturges*, J. H. (2004): Comparing telephone and face-to-face qualitative interviewing: a research note. Qual. Res., 4(1), S. 107 – 118.

*Tøndel*, I. M. (2015): Using Cyber-Insurance as a Risk Management Strategy: Knowledge Gaps and Recommendations for Further Research. Abgerufen im Januar 2024 von SINTEF ICT: https://brage.bibsys.no/xmlui/bitstream/handle/11250/2379189/SINTEF%2bA27298.pdf?sequence=3&isAllowed=y.

*Tosh*, D. S. (2017): Risk management using cyber-threat information sharing and cyber-insurance. (S. A. L., Hrsg.) USA: Springer.

*Tsohou*, A. (16.1.2023): Cyber insurance: state of the art, trends and future directions. International Journal of Information Security, 22(3), S. 737 – 748.

*Völz*, H.-J. (2018): Der Mittelstand BVMW. Abgerufen im Januar 2024 von https://www.bvmw.de/uploads/topics/Unternehmertum/Downloads/KMU-Definition.pdf.

*Woods*, D. S. (2017): Policy measures and cyber insurance: a framework. J. Cyber Policy, 2(2), S. 209 – 226.

*Wrede*, D. F.-M. (2018): Herausforderungen und Implikationen für das Cyber-Risikomanagement – Eine empirische Analyse. Z. Ges. Versicherungswiss., 107(4).

*Yin*, R. (2014): Case Study Research: Design and Methods. SAGE.

*Zhao*, X. X. (2013): Managing interdependent information security risks: cyberinsurance, managed security services, and risk pooling arrangements. J. Manage. Inf. Syst., 30(1), S. 123 – 152.