Cyber-Risiko-Management – Eine empirische Analyse über Einflussfaktoren und die Quantifizierung von Cyber-Angriffen

Inauguraldissertation
zur Erlangung des akademischen Grades eines Doktors
der Wirtschaftswissenschaften des Fachbereichs Wirtschaftswissenschaften
der Universität Osnabrück

vorgelegt von

Bennet Simon von Skarczinski, M. Sc.

Osnabrück, Juni 2024

Dekan:	Prof. Dr. Frank Teuteberg
Referenten:	Prof. Dr. Frank Teuteberg
	Prof. Dr. Oliver Thomas
Tag der Disputation:	11.06.2024

Vorwort

Die vorliegende Dissertation ist im Rahmen meiner Forschung als externer Doktorand im Fachgebiet Unternehmensrechnung und Wirtschaftsinformatik (UWI) am Institut für Informationsmanagement und Unternehmensführung (IMU) im Fachbereich Wirtschaftswissenschaften der Universität Osnabrück entstanden. Während dieser Zeit durfte ich das Forschungsprojekt „Cyberangriffe gegen Unternehmen“ als assoziierter Projektmitarbeiter am Kriminologischen Forschungsinstitut Niedersachsen (KFN) von Dezember 2017 bis März 2021 begleiten. Neben meinen Beratungsprojekten im Bereich Cybersecurity & Privacy hat mir mein Arbeitgeber PricewaterhouseCoopers GmbH WPG (PwC) Arbeitszeit und weitere Unterstützung für die Beteiligung am Forschungsprojekt „Cyberangriffe gegen Unternehmen“ zur Verfügung gestellt. Ohne die breite, positive und immer aufbauende Unterstützung durch ein tragendes privates und berufliches Netzwerk wäre diese Dissertation nicht möglich gewesen. Daher muss ich nun etlichen Menschen danken.

Ich möchte meinem Doktorvater Prof. Dr. Frank Teuteberg für seine wertvolle Betreuung, die vielen guten Hinweise und Anmerkungen sowie für die immer freundliche und responsive Kommunikation danken. Sein Einsatz und seine Unterstützung, auch im Beirat des KFN-Forschungsprojektes, haben mir viel bedeutet. Ich danke zudem Prof. Dr. Thomas für die Übernahme des Koreferats dieser Dissertation. Bedanken möchte ich mich auch bei den (ehemaligen) Mitarbeitern und Mitarbeiterinnen des Fachgebiets UWI, insbesondere Dr. Michael Adelmeyer, Dr. Eduard Anton und Marita Imhorst für die vielen Tipps und Hilfen formaler und organisatorischer Natur. Derselbe Dank gilt den Mitarbeiterinnen des Dekanats, insb. Frau Jatzkowski und Frau Levinsky.

Mit Blick auf meine bereichernde Zeit am KFN möchte ich mich bei Prof. Dr. Christian Pfeiffer und Prof. Dr. Gina Rosa Wollinger für die Initiierung des Forschungsprojektes, das erfolgreiche Vorstellungsgespräch und die vielen guten Diskussionen und Ideen sowie die ein oder andere Tasse Tee bedanken. Arne Dreißigacker, was soll ich sagen? Ohne dich und deine gutmütige, analytische und fortwährende Unterstützung wäre vieles schiefgelaufen. Vielen Dank für die tolle und freundschaftliche Zusammenarbeit in den letzten Jahren. Darüber hinaus danke ich den (ehemaligen) Doktoranden und Mitarbeitenden des KFN für die vielen wichtigen Diskussionen fachlicher und methodischer Natur sowie für etliche unvergessliche Erlebnisse (u.a. Sommerfeste in der Justizvollzugsanstalt, der Pastrami-Donnerstag, Portwein-Freitage, etc.). Ich möchte mich auch bei Prof. Dr. Sascha Fahl, Nicolas Huaman und Dr. Christian Stransky von der Leibniz Universität Hannover bzw. dem CISPA Helmholtz-Zentrum für Informationssicherheit Hannover für die spannende Zusammenarbeit im Rahmen des Forschungsprojektes bedanken. Mein tiefster Dank gilt zudem meinen noch nicht erwähnten Koautoren: Dr. Marie Christine Bergmann, Dr. Dominik Wermke, Prof. Dr. Yasemin Acar, Lukas Boll und Dr. Mathias Raschke. Insbesondere Mathias danke ich für die vielen, aus Rücksicht auf die „Ins-Bett-Geh-Zeit der Kinder“, spät-abendlichen Telefonate und Diskussionen.

Ohne die gewährte Flexibilität und Unterstützung von PwC wäre diese Dissertation in dieser Form nicht möglich gewesen. Ich möchte mich daher ausdrücklich bei Thomas Stieve und Joachim

Mohs für die Ermöglichung der Teilnahme meiner Person an dem KFN-Forschungsprojekt bedanken. Danke Joachim für dein Vertrauen und deine anspruchsvolle und kontinuierliche Forder- und Förderung. An den vielen herausfordernden Projektsituationen, Priorisierungs- und Steuerungsaufgaben bin ich stark gewachsen. Ich danke zudem den zahlreichen PwC-Kolleginnen und Kollegen, die mich auf meinem Weg durch viele Gespräche, Ideen und Taten unterstützt haben: Nial Moore, Tobias Franz Langkau, Grant Waterfall, Stefanie Otersen, Henning Kruse, Dr. Thierry Ruch, Friederike Erdmann, Robert Schamber und die vielen anderen. Ich danke zudem Peter Reipen für sein Mentoring in meinen ersten PwC-Jahren sowie seine Unterstützung, mich vom Finanz-Risiko-Management zum Cyber-Risiko-Management entwickeln zu können.
Mein privates Umfeld hat mich in den letzten Jahren getragen und mir Kraft für die vielen herausfordernden aber auch schönen Tage gegeben. Liebe Freunde und Familie, bitte entschuldigt die zahlreichen zeitlichen Restriktionen für gemeinsame Treffen und Aktivitäten. Ich danke euch umso mehr für euer Verständnis und eure unveränderte Unterstützung. Danke Caleb and Kyla Addie für das Mitfiebern und das Korrekturlesen einiger englischsprachiger Beiträge. Ich danke meinen liebevollen Eltern Uta und Matthias sowie meinen großartigen Geschwistern Anne und Jannes für eure bedingungslose Unterstützung und eure Fürsorge seitjeher. Zu guter Letzt, möchte ich mich ausdrücklich bei meiner Frau Ina und meinen Kindern Leonora, Pauline und Matilda für euer Verständnis, die Rücksichtnahme, den familiären Rückhalt, eure Liebe und euer Vertrauen bedanken.

Wennigsen (Deister) / Bredenbeck, Juni 2024
Bennet von Skarczinski

Inhaltsverzeichnis

Teil B – Forschungsbeiträge VII

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

AG	Aktiengesellschaft
AIC	Akaike Information Criterion
AIS	Association for Information Systems
BCM	Business Continuity Management
BMWi	Bundesministerium für Wirtschaft und Energie
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVMW	Bundesverband mittelständische Wirtschaft
BYO	Bring your own (device)
CapEx	Capital Expenditures
CATI	Computer Assisted Telephone Interview
CSMS	Cyber Security Management System
CV	Cyber-Versicherung
DORA	Digital Operational Resilience Act
DPMS	Data Privacy Management System
DSGVO	Datenschutzgrundverordnung
ECIS	European Conference on Information Systems
GPD	Generalized Pareto Distribution
GEV	Generalized Extreme Value Distribution
HSPV NRW	Hochschule für Polizei und öffentliche Verwaltung Nordrhein-Westfalen
IHK	Industrie- und Handelskammer
IS	Informationssicherheit / information security
ISMS	Information Security Management System
KFN	Kriminologisches Forschungsinstitut Niedersachsen
KI	Künstliche Intelligenz
KMU	Kleine- und mittelständische Unternehmen
KPI	Key Performance Indicator
LKA	Landeskriminalamt
NDS	Niedersachsen
OpEx	Operational Expenditures
PLS-PM	Partial Least Squares Path Modelling
PwC	PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft
SIEM	Security Information and Event Management (System)
SH	Schleswig-Holstein
SOC	Security Operations Center
WI	Wirtschaftsinformatik
VHB	Verband der Hochschullehrer für Betriebswirtschaftslehre
VHB JQ3	VHB Journal Quality Index 3
WKWI	Wissenschaftliche Kommission Wirtschaftsinformatik
WZ08	Klassifikation der Wirtschaftszweige, Ausgabe 2008

Teil A – Dachbeitrag

1 Einleitung

1.1 Ausgangssituation

Neben den zahlreichen Vorzügen der zunehmenden Digitalisierung und Vernetzung unternehmerischer Wertschöpfungsketten birgt diese Entwicklung auch Herausforderungen für Unternehmen (Legner et al. 2017). So gelten Cyber-Risiken unter Geschäftsführenden und Risiko-Managern noch vor makroökonomischen, energie- oder klima-bedingten Risiken weltweit als die dominierenden Geschäftsrisiken (Allianz 2023, 2022). Cyber-Risiken definieren sich als das Potential, dass eine gegebene Bedrohung, die im Cyber-Raum existiert oder zeitweise dort präsent ist, Schwachstelle(n) ausnutzt, um Vermögenswerte bzw. Cyber-Ressourcen zu kompromittieren und somit einer Organisation Schaden zufügt (ENISA 2023; NIST 2023). Die Schutzziele der Informationssicherheit - Vertraulichkeit, Integrität und Verfügbarkeit von Informationen, Daten, Systemen und Prozessen - sind damit gefährdet (ENISA 2017).

Die betrieblichen Ökosysteme, in denen Unternehmen entlang ihrer Wertschöpfungsketten agieren, sind dynamisch und hoch komplex (Rüegg-Stürm 2013). Unter Einfluss verschiedener Umweltsphären und Stakeholdern führen Unternehmen im Rahmen ihrer betrieblichen Funktionen Management-, Geschäfts- und Unterstützungsprozesse aus (Rüegg-Stürm 2013). Aus Effizienz- und Standardisierungsgründen nimmt die Fertigungstiefe ab und die Arbeitsteilung entlang der Wertschöpfung zu (Rüegg-Stürm 2013). Das hat zur Folge, dass betriebliche Prozesse stark untergliedert sind und von einer Vielzahl von Systemen, organisatorischen Kontexten und ausführenden (dritten) Personen unterstützt werden, die Informationen über verschiedene Schnittstellen austauschen. Abbildung 1 stellt eine Auswahl cyber-risiko-relevanter Einflussfaktoren auf das betriebliche Ökosystem dar und skizziert damit die Herausforderungen, mit denen sich Unternehmen im Rahmen des Cyber-Risiko-Managements konfrontiert sehen.

In der Domäne der politischen Einflussfaktoren führte beispielsweise der Angriffskrieg auf die Ukraine und die Warnung des Bundesamtes für Sicherheit in der Informationstechnik (BSI 2022) dazu, dass die Nutzung russischer Sicherheitssoftware durch westliche Unternehmen schlagartig reduziert wurde (Matthiesen 2022). Dies hatte nicht nur hohe Umstellungsaufwände zur Folge, sondern demonstrierte auch, wie aus sicher geglaubten Prozessen und Systemen unvermittelt neue Bedrohungen entstehen können, die im Rahmen des Cyber-Risiko-Managements behandelt werden müssen. Weitere politische Einflussfaktoren sind beispielweise neue Regularien wie die EU-NIS-2 Richtlinie (EU 14.12.2022) oder der EU-Cyber-Resilience-Act (EU-Commission 2023), welche fordern, dass mehr europäische Unternehmen stärkere Cyber-Sicherheitsmaßnahmen, unter anderem in den Bereichen Cyber-Risiko-Management, Kontrolle, Überwachung und Meldung, Business-Continuity-Management sowie Incident-Management und Produktsicherheit entlang ihrer Wertschöpfungsketten etablieren (Openkritis 2023). Neben weiteren ökonomischen, sozio-kulturellen, technologischen und rechtlichen Einflussfaktoren sind Unternehmen insbesondere von der Digitalisierung der Kriminalität betroffen. Künstliche Intelligenz (KI) verändert die Geschwindigkeit und die Art und Weise mit der Cyber-Angriffe vorbereitet und durchgeführt werden können (Guembe et al. 2022). Durch sog. Crime-as-a-Service-Angebote können Täter und Täterinnen auch ohne größeres technisches Wissen effektive Angriffe ausführen und

versuchen, die zunehmenden digitalen Vermögenswerte von Unternehmen zu erbeuten (BKA 2022). Demgegenüber stehen rückläufige Aufklärungsquoten aufgrund verstärkter Anonymisierungsmöglichkeiten oder im Ausland agierender Täter und Täterinnen, was das sog. Cybercrime mitunter besonders attraktiv erscheinen lässt (BKA 2022).

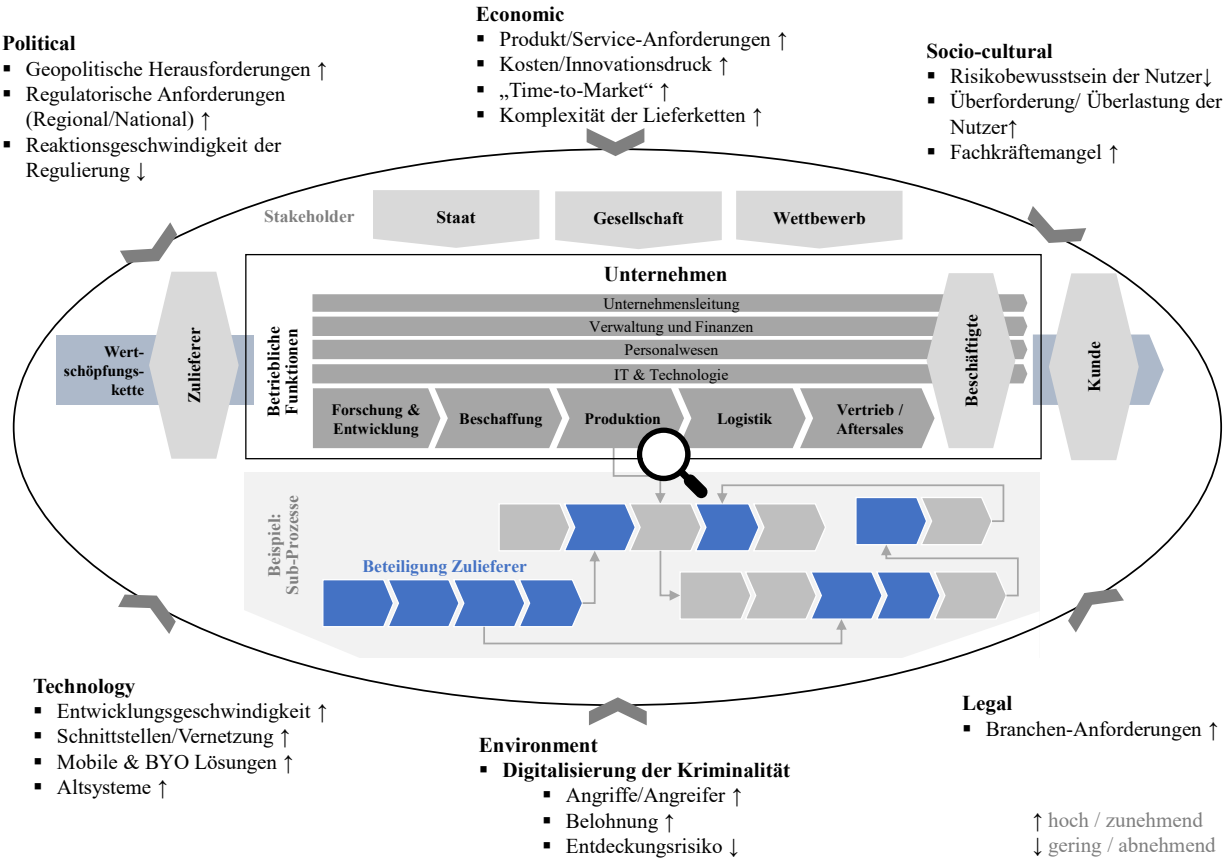

Abb. 1: Exemplarische Auswahl Cyber-Risiko relevanter Einflussfaktoren auf das betriebliche Ökosystem nach PESTEL-Dimensionen (eigene Darstellung nach: Fahey und Narayanan 1986; Rüegg-Stürm 2013; Thommen und Achleitner 2012).

Die Aufgabe des betrieblichen Cyber-Risiko-Managements ist es, die aus den verschiedenen Einflussfaktoren auf das betriebliche Ökosystem wirkenden Risiken systematisch zu identifizieren, zu analysieren, zu bewerten/quantifizieren, zu behandeln und fortlaufend zu überwachen (ISO/IEC 27005:2022(en)). Dieses komplexe Gemenge aus "technological and social interactions embedded in an organizational setting" (Cresswell und Hassan 2007) führt zu einem vielschichtigen und dynamischen Handlungs- und Forschungsfeld.

1.2 Motivation und Zielsetzung

Um in Zeiten der Digitalisierung bestehen und sich positiv entwickeln zu können, müssen Unternehmen ihre Cyber-Risiken identifizieren, bewerten und aktiv steuern. Neben dem Eigeninteresse der Geschäftsfortführung fordern dies auch immer mehr einschlägige Regularien[1] und Standards[2]. In Kongruenz dazu hat in den letzten Jahren auch die Forschung im Bereich

[1] z.B. IT-Sicherheitsgesetz 2.0; EU-NIS 2; EU-Cyber Resilience Act; EU Digital Operational Resilience Act (DORA); UN Regulation Nr. 155; §91 Aktiengesetz; EU-DSGVO
[2] z.B. ISO 2700x Reihe; BSI IT-Grundschutz; ISO 21434

Informationssicherheits-Management und Cyber-Risiko-Management stark zugenommen (Herath et al. 2020). Bisherige Forschung im Bereich Informationssicherheits-Management fokussiert auf konzeptionelle Beiträge, das Verhalten von Individuen oder ökonomische/volkswirtschaftliche Perspektiven (Herath et al. 2020). Forschung im Bereich der Investitionen in Informationssicherheit basiert auf vor allem auf mikroökonomischen Ansätzen auf der Grundlage der Spieltheorie, Finanzanalysen auf der Grundlage von Kapitalrenditen und Kapitalwerten oder Managementansätzen auf der Grundlage der Entscheidungstheorie (Weishäupl und Yasasin 2015; Weishäupl et al. 2018). Doch gerade mit Blick auf das betriebliche Cyber-Risiko-Management bestehen wesentliche Forschungslücken (Eling 2020). Der Mangel an verlässlichen empirischen Daten stellt nach wie vor eine große Herausforderung dar (Marotta et al. 2017; Wolff und Lehr 2017; EIOPA 2018; Romanosky et al. 2019; Dambra et al. 2020; Eling 2020; Wrede et al. 2020; Buil-Gil et al. 2021; Wheatley et al. 2021; Cremer et al. 2022). Es existieren wenig empirisch orientierte Organisationsstudien, die Management-Perspektiven der Informationssicherheit einnehmen (Herath et al. 2020), und bisherige Ansätze zur Entscheidungsfindung im Cyber-Risiko-Management sind zudem meist reaktiv und qualitativ orientiert (Pate-Cornell und Kuypers 2021). Hingegen sind Studien, die „real world compromises or harm affecting organizations“ und deren erklärenden Determinanten empirisch untersuchen und quantifizieren selten und werden dringend benötigt (Woods und Böhme 2021). Eling (2020) subsumiert daher, dass die Cyber-Risiko-Forschung noch in den Kinderschuhen steckt, weil noch „so viel mehr getan werden muss“, um diesen immer wichtigeren Teil der Wirtschaft und Gesellschaft zu verstehen.
Aufgrund der aufgezeigten Bedarfe ist die Zielsetzung der vorliegenden Dissertation, empirische Einflussfaktoren und Zusammenhänge von Cyber-Angriffen zu identifizieren und zu analysieren sowie deren Auswirkungen zu quantifizieren, um ein betriebliches Cyber-Risiko-Management zu unterstützen. Die vorliegende Dissertation ist im Kontext des Forschungsprojektes „Cyberangriffe gegen Unternehmen“[3] des Kriminologischen Forschungsinstitutes Niedersachsen (KFN) entstanden und hat einen vorwiegend betriebswirtschaftlichen Fokus auf das Phänomen Cyber-Risiko-Management. Die mit dieser Arbeit gewonnenen Erkenntnisse sind grundlegend und basieren auf einem eher positivistischen, quantitativen Forschungs-Paradigma (vgl. Straub und Gefen 2004; Myers 1997). Sie sollen Forschende und Unternehmen darin unterstützen, Ansätze und Methoden zu entwickeln, um informierte, effiziente und wirtschaftliche Entscheidungen im Rahmen des betrieblichen Cyber-Risiko-Managements treffen zu können.

1.3 Aufbau der kumulativen Dissertation

Der Aufbau dieser kumulativen Dissertation ist zweigeteilt. Teil A bildet mit seinen fünf Kapiteln den Dachbeitrag. Nach der einleitenden Beschreibung der Ausgangssituation, Motivation und Zielsetzung der Dissertation stellt das zweite Kapitel die inhaltliche und methodische Verortung der Forschungsbeiträge dar. Im dritten Kapitel werden die wesentlichen Ergebnisse der Forschungsbeiträge zusammengefasst und die Implikationen und weiteren Forschungsbedarfe anschließend im vierten Kapitel diskutiert. Zuletzt erfolgt das Fazit im fünften Kapitel. Teil B führt die Forschungsbeiträge der kumulativen Dissertation auf und fasst die bibliographischen Informationen der Beiträge in jeweils einer Tabelle zusammen.

[3] Kriminologisches Forschungsinstitut Niedersachsen (KFN); Weitere Informationen zum Forschungsprojekt unter: https://kfn.de/forschungsprojekte/cyberangriffe-gegen-unternehmen/

2 Forschungs-Design

2.1 Kontext: Forschungsprojekt „Cyberangriffe gegen Unternehmen“

Die Forschungsbeiträge der vorliegenden Dissertation sind im Bezugsrahmen des KFN-Forschungsprojektes „Cyberangriffe gegen Unternehmen“ entstanden. In der Projektlaufzeit vom Dezember 2017 bis März 2021 wurden in Zusammenarbeit mit dem Forschungszentrum L3S der Leibniz Universität Hannover zehn Arbeitspakete abgeleistet (siehe Dreißigacker et al. 2020b, 15 ff.). Neben der Erhebung des Forschungsstandes, der Durchführung von Experteninterviews zur Einordnung des Phänomens, der Erstellung einer Vorhersage-Plattform und verschiedener Feldstudien, u.a. zur Benutzbarkeit von Security Information and Event Management Systemen (SIEM) oder der Evaluation von IT-Sicherheitsdokumentationen wurde insbesondere eine CATI-Befragung (Computer Assisted Telephone Interviews) von 5.000 deutschen Unternehmen sowie eine webbasierte Folgebefragung durchgeführt.

Das Projekt wurde vom Bundesministerium für Wirtschaft und Energie (BMWi) gefördert und erhielt eine Zusatzförderung von der PricewaterhouseCoopers GmbH WPG (PwC) sowie der VHV Stiftung. Die Förderung durch PwC beinhaltete die Entsendung des Autors der vorliegenden Dissertationsschrift als assoziierten Projektmitarbeiter an das KFN. Daneben beteiligten sich Experten und Expertinnen verschiedener Kooperationspartner am Forschungsprojekt (u.a. Wirtschaftsschutz/Verfassungsschutz NDS., Landeskriminalamt NDS., Bundesverband mittelständische Wirtschaft (BVMW), IHK Hannover, PwC, HSPV NRW).

Fünf der sechs Beiträge der vorliegenden Dissertation nutzen Vorarbeiten und Daten des oben genannten Forschungsprojektes. Sie haben ferner einen betriebswirtschaftlichen Fokus auf das Phänomen Cyber-Risiko, während andere projektbezogene Publikationen eher kriminologische oder technologische Perspektiven einnehmen. Innerhalb der Projektlaufzeit nahm der Autor am regelmäßigen Doktoranden-Kolloquium des KFN teil, um die Forschungsbeiträge fachlich und methodisch mit den interdisziplinär Promovierenden des KFN zu diskutieren.

2.2 Auswahl der Forschungsbeiträge

Im Zeitraum von 2017 bis 2023 wurden zahlreiche wissenschaftliche und fachspezifische Publikationen zum Thema Cyber-Angriffe und Cyber-Risiken durch den bzw. unter Beteiligung des Autors erstellt. In die vorliegende Dissertation gehen die sechs in Tabelle 2 genannten Forschungsbeiträge ein. Alle aufgeführten Forschungsbeiträge durchliefen jeweils einen doppelt-blinden Begutachtungsprozess, in dem zwei bis fünf Gutachter bzw. Gutachterinnen die Beiträge mit Bezug auf Inhalt und Methodik kritisch würdigten. Die weiteren Publikationen, die nicht dem für eine Dissertation üblichen Publikationstyp bzw. Veröffentlichungsprozess entsprechen, wurden aus Informationsgründen im Anhang A aufgelistet.

Beitrag	Bibliographische Informationen	Medium	Ranking
A	Bergmann, Marie Christine; Dreißigacker, Arne; **von Skarczinski, Bennet Simon**; Wollinger, Gina Rosa (2018) *[1]: Cyber-Dependent Crime Victimization: The Same Risk for Everyone? In: Cyberpsychology, behavior and social networking [Mary Ann Liebert]	Journal	▪ **Q1** (SJR 1,466)[4] ▪ **8,7** (CiteScore; Top 94 Perzentil)[5]
B	Huaman, Nicolas; **von Skarczinski, Bennet Simon**; Wermke, Dominik; Stransky, Christian; Acar, Yasemin; Dreißigacker, Arne; Fahl, Sascha (2021) *[2]: A Large-Scale Interview Study on Information Security in and Attacks against Small and Medium-sized Enterprises. In: Proceedings of the 30th USENIX Security Symposium	Konferenz	▪ **A*** (CORE)[6] ▪ **Tier 1** (TAMU)[7]
C	**von Skarczinski, Bennet Simon**; Boll, Lukas; Teuteberg, Frank (2021) *[3]: Understanding the adoption of cyber insurance for residual risks - An empirical large-scale survey on organizational factors of the demand side. In: European Conference on Information Systems (ECIS) Proceedings [AIS]	Konferenz	▪ **A** (WKWI) ▪ **B** (VHB JQ3) ▪ **A** (VHB Rating 2024)
D	**von Skarczinski, Bennet Simon**; Dreißigacker, Arne; Teuteberg, Frank (2022) *[4]: Toward enhancing the information base on costs of cyber incidents: implications from literature and a large-scale survey conducted in Germany. In: Organizational Cybersecurity Journal (OCJ) [Emerald]	Journal	▪ Kein Ranking / Score verfügbar
E	**von Skarczinski, Bennet Simon**; Dreissigacker, Arne; Teuteberg, Frank (2022) *[5]: More Security, less Harm? Exploring the Link between Security Measures and Direct Costs of Cyber Incidents within Firms using PLS-PM. In: Wirtschaftsinformatik (WI) 2022 Proceedings (2) [AIS]	Konferenz	▪ **A** (WKWI) ▪ **C** (VHB JQ3) ▪ **B** (VHB Rating 2024)
F	**von Skarczinski, Bennet Simon**; Raschke, Mathias; Teuteberg, Frank (2023) *[6]: Modelling maximum cyber incident losses of German organisations: an empirical study and modified extreme value distribution approach. In: The Geneva Papers on Risk and Insurance - Issues and Practice [Palgrave Macmillan / Springer Nature]	Journal	▪ **B** (VHB JQ3) ▪ **B** (VHB Rating 2024)

Kommentare:
* Prof. Dr. Frank Teuteberg ist Co-Autor der Beiträge C – F und reflektierte die inhaltliche und methodische Ausrichtung der Beiträge kritisch
*[1] Die Autorinnen und Autoren arbeiteten in gleichen Teilen an dem Beitrag
*[2] Herr Nicolas Huaman übernahm wesentliche Anteile der Texterstellung sowie der Datenauswertung. Herr Dominik Wermke und Herr Christian Stransky unterstützten in der Datenanalyse sowie im Schreiben und der Revision von Texten. Frau Prof. Dr. Jasmin Acar unterstützte im Schreiben und der Revision von Texten. Herr Arne Dreißigacker übernahm wesentliche Anteile in der Datenerhebung/Datenvorbereitung. Prof. Dr. Sascha Fahl reflektierte die inhaltliche und methodische Ausrichtung des Beitrags kritisch
*[3] Herr Lukas Boll übernahm wesentliche Anteile in der Datenauswertung
*[4] *[5] Herr Arne Dreißigacker übernahm wesentliche Anteile in der Datenerhebung/Datenvorbereitung sowie in der Revision der Inhalte
*[6] Herr Dr. Mathias Raschke übernahm die Herleitung und Konzeption der Verteilungsmodelle und Anwendungsbespiele sowie die Revision der Inhalte und schrieb Teile der Texte

Tab. 1: Übersicht der Forschungsbeiträge.

Die sechs für diese Dissertation relevanten Forschungsbeiträge wurden in englischer Sprache

[4] SCImago Journal Rank Indicator SJR = 1,466 (232 von 1956; 11,9%; Q1) in Computer Science Journals; https://www.scimagojr.com/journalrank.php?area=1700 (04.07.2023)
[5] Scopus CiteScore: 8,7 (94th percentile in Social Psychology Journals 2022); https://www.scopus.com/sourceid/19700176047 (04.07.2023)
[6] CORE Ranking 2021: A* - flagship conference, a leading venue in a discipline area (7.45% of 792 ranked venues); http://portal.core.edu.au/conf-ranks/?search=USenix&by=all&source=CORE2021&sort=atitle&page=1 (04.07.2023)
[7] Texas A&M University, Security Conference Ranking and Statistic (Annahmequote USENIX Security Symposium 2022: 18,1%); https://people.engr.tamu.edu/guofei/sec_conf_stat.htm (07.04.2023)

verfasst, um die internationale Sicht- und Nutzbarkeit zu gewährleisten. Fünf der sechs Beiträge wurden in hochrangigen Publikationsorganen veröffentlicht, für welche jeweils einschlägige Rankings als Indikation für die wissenschaftliche Qualität der Konferenzen und Journals zur Verfügung stehen. Da das Thema Cyber-Risiko auch stark in den Disziplinen Informatik, Computer Science und Kriminologie verankert ist, liegen nicht für alle Publikationsorgane der Forschungsbeiträge Rankings des Verbandes der Hochschullehrerinnen und Hochschullehrer für Betriebswirtschaftslehre (VHB 2022) oder der Wissenschaftlichen Kommission Wirtschaftsinformatik (WKWI) (Heinzl et al. 2008) vor. In diesem Fall wird auf alternative Rankings und Kennzahlen benachbarter bzw. übergreifender Disziplinen zurückgegriffen. So wurde Beitrag A im renommierten Journal „Cyberpsychology, behavior and social networking“ veröffentlicht, für welches ein Scopus CiteScore sowie ein SCImago Journal Rank Indicator vorhanden sind. Beitrag B wurde auf einer der führenden IT-Security Konferenzen, USENIX Security Symposium, veröffentlicht, für die ein CORE-Rating vorliegt sowie Statistiken durch Angehörige der Texas A&M University geführt werden.
Für das Publikationsorgan des Beitrages D liegen derzeit noch keine Rankings vor, was daran liegen dürfte, dass das Organizational Cybersecurity Journal (OCJ) neugegründet wurde, und die Erstausgabe 2021 erschien. Das OCJ erscheint im renommierten Emerald Verlag und wird von bekannten Indexing Services gelistet (z.B. EBSCO Discovery, Google Scholar, WorldCat). Die Universität von Colorado (USA) - Colorado Springs College of Business and Cybersecurity Management Council sponsort das OCJ, welches von Prof. Dr. Gurvirender Tejay als Editor-in-Chief geleitet wird. Die Gutachter und Gutachterinnen des OCJ stammen überwiegend von renommierten Universitäten aus den Vereinigten Staaten von Amerika (Emerald Publishing 2023), darunter auch die Senior Editors Prof. Dr. John D'Arcy, University of Delaware, und Prof. Dr. Mikko Siponen - University of Jyväskylä, Finnland, die selbst zahlreiche Beiträge in VHB JQ3 A-gerankten Publikationsorganen veröffentlicht haben (z.B. MIS Quarterly, European Journal of Information Systems (EJIS), Information Systems Research (ISR)).
Im folgenden Kapitel wird nun auf die inhaltliche Verortung und Einordnung der Forschungsbeiträge eingegangen.

2.3 Rahmenwerk der Beiträge und Forschungsfragen

Die Zielsetzung der vorliegenden Dissertation ist, empirische Einflussfaktoren und Zusammenhänge von Cyber-Angriffen zu identifizieren und zu analysieren sowie deren Auswirkungen zu quantifizieren, um ein betriebliches Cyber-Risiko-Management zu unterstützen. Abbildung 2 fasst die Einordnung der Beiträge in dieser Hinsicht grafisch zusammen.
Die Ziele der Informationssicherheit einer Organisation werden in der Regel durch sog. Managementsysteme verfolgt und adressiert. Managementsysteme werden definiert als die Gesamtheit aller organisatorischen, technischen und personellen Regelungen, Maßnahmen, Vorgaben, Prozesse, Kapazitäten und Fähigkeiten, die systematisch gesteuert und verbessert werden, um bestimmte Ziele einer Organisation zu definieren und zu erreichen (vgl. DIN EN ISO 9000:2015; BSI 2021, ISMS.1 Sicherheitsmanagement). Managementsysteme mit Bezug zur Informationssicherheit haben verschiedene Wirkungsbereiche und können sich auf die Organisation selbst (z.B. Informationssicherheitsmanagementsystem (ISMS) nach ISO27001), bestimmte Produkte oder Services (z.B. Cybersecurity-Managementsystem (CSMS) für

Automobile nach UNECE Regulation 155), bestimmte Daten (z.B. Data Privacy Management System (DPMS) zum Schutz personenbezogener Daten nach EU-DSGVO) oder auch andere thematische Schwerpunkte (z.B. Business Continuity Management ISO22301) beziehen. Das Cyber-Risiko-Management hingegen kann diese Managementsysteme mit Aussagen zu bestehenden Cyber-Risiken sowie deren Eintrittswahrscheinlichkeiten und potentiellen Schadensausmaß unterstützen.

Im Rahmen dieser Dissertation wird das Cyber-Risiko-Management in zwei Teilbereiche mit unterschiedlichen Zielsetzungen unterteilt: Erstens in die Systematisierung von Cyber-Risiken und zweitens in die Quantifizierung von Cyber-Risiken. In dem ersten Teilbereich „Systematisierung" wird das Ziel verfolgt, Einflussfaktoren und mögliche Kausalzusammenhänge von Cyber-Risiken zu verstehen. Das Kausalmodel von Woods und Böhme (2021) bietet dazu eine geeignete Grundlage. Demnach führen Cyber-Bedrohungen (Threats) zu Kompromittierungen (Compromise), welche sich als Verletzung betrieblicher Schutzziele der Informationssicherheit mit Hinblick auf die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen definieren. Die Wirkung von „Threat" auf „Compromise" wird dagegen insofern durch präventive Sicherheitsmaßnahmen moderiert, als das mehr implementierte präventive Sicherheitsmaßnahmen die Wirkung reduzieren. Schwachstellen und mehr sog. Angriffsfläche (Surface Exposure) verstärken den Effekt von „Threat" auf „Compromise". Im nächsten Schritt führt „Compromise" zu Schäden (Harm), wobei auch diese Beziehung durch reaktive Sicherheitsmaßnahmen moderiert wird. Das Vorhandensein von Vermögensgegenständen (Asset Exposure), die durch einen „Compromise" beeinträchtigt (z.B. zerstört, manipuliert, entwendet) werden können, verstärkt hingegen den Effekt von „Compromise" auf „Harm". Dieses Modell kann aus differenzierten Perspektiven betrachtet werden, die eher technologisch, organisatorisch bzw. prozessual oder verhaltenswissenschaftlich geprägt sind, aber im Zusammenfluss gesehen werden müssen, um Informationssysteme ganzheitlich zu erfassen (Hevner et al. 2004).

In dem zweiten Teilbereich „Quantifizierung" wird das Ziel verfolgt, die eigentlichen Cyber-Risiken, im Sinne von Eintrittswahrscheinlichkeiten und potenziellen Schadensausmaßen, zu ermitteln und durch evidenzbasierte Schlussfolgerungen die betrieblichen Steuermechanismen zu unterstützen. Für einen definierten Geltungsbereich (Scope; z.B. bestimmte Systeme, Prozesse, Daten, Infrastruktur, rechtliche Einheiten, etc.) können mithilfe geeigneter Daten (z.B. externe Bedrohungsdaten, Reifegrad-Assessments, Incident-Daten, Controlling-Daten, etc.) verschiedene Methoden zur Quantifizierung von Cyber-Risiken angewandt werden. Im Rahmen dieser Dissertation werden deskriptive Statistik und Gruppenvergleiche sowie Methoden der stochastischen Modellierung eingesetzt, um Cyber-Risiken zu quantifizieren. Da die in den Forschungsbeiträgen angewendeten Methoden danach streben „to develop and justify theories (i.e., principles and laws) that explain or predict organizational and human phenomena surrounding the analysis, design, implementation, management, and use of information systems", sind sie vornehmlich dem Behavioral-Science-Paradigma mit Wurzeln in den Naturwissenschaften zuzuordnen (Hevner et al. 2004).

Mit Blick auf die Verortung der Forschungsbeiträge fokussieren die Beiträge A, B, C und E die Untersuchung von ausgewählten Faktoren und Zusammenhängen. In den Beiträgen D und F steht die eigentliche Quantifizierung von Risiken im Vordergrund.[8]

[8] Aufgrund der Begutachtungs- und Veröffentlichungsprozeduren stimmt die Reihenfolge der nummerierten Beiträge nicht vollständig mit der Chronologie der Erstellungszeiträume und Veröffentlichungsdaten überein.

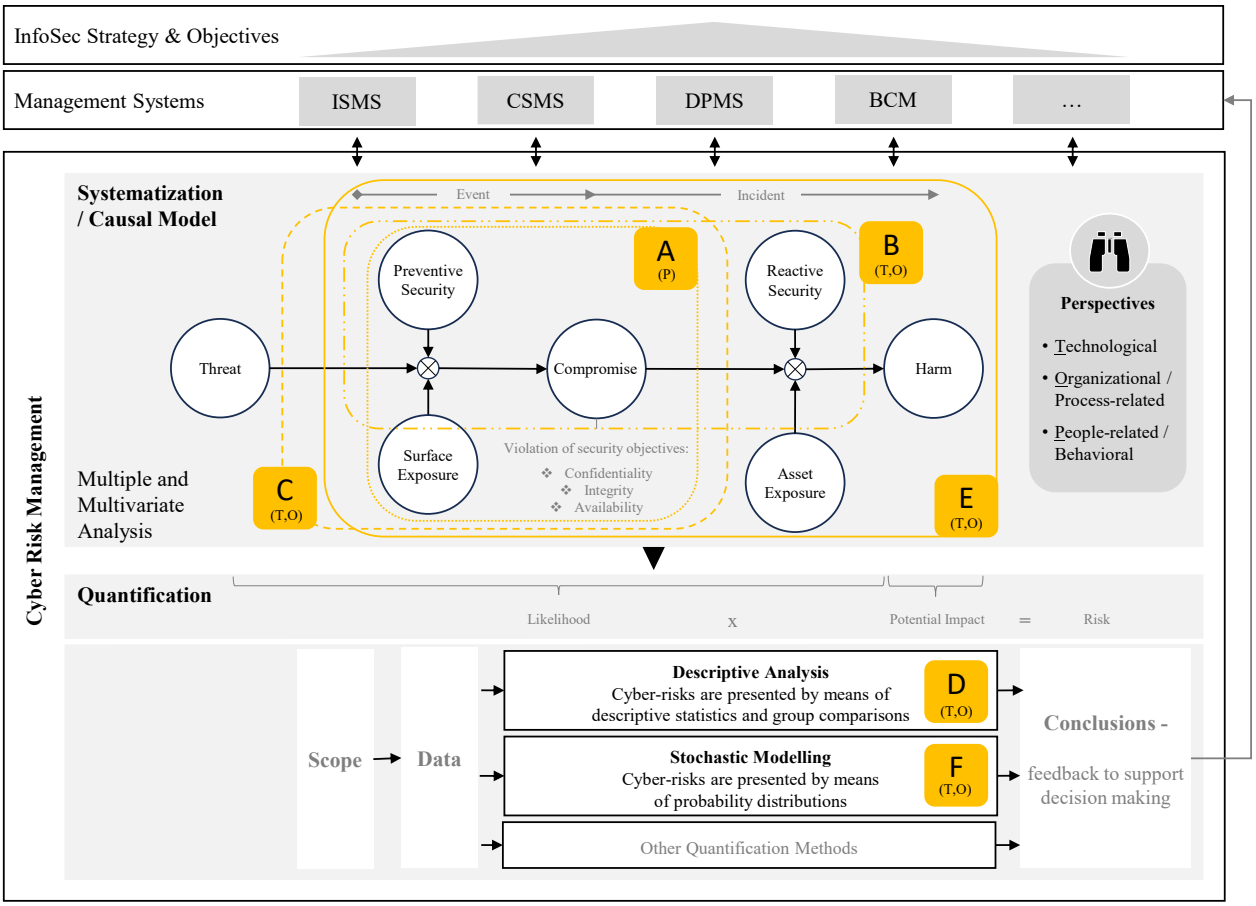

Abb. 2: Einordnung der Forschungsbeiträge (eigene Darstellung; Kausalmodell nach Woods und Böhme 2021).

Der **Beitrag A** *„Cyber-Dependent Crime Victimization: The Same Risk for Everyone?"* (Bergmann et al. 2018) untersucht die Forschungsfrage, welche individuellen und kontextuellen Merkmale die Cyber-Viktimisierung mit Blick auf verschiedene Deliktarten beeinflussen. Damit nimmt der Beitrag eine eher kriminologische bzw. sozialwissenschaftliche Perspektive auf die Modellvariablen „Preventive Security", „Surface Exposure" und „Compromise" ein.

Der **Beitrag B** *„A Large-Scale Interview Study on Information Security in and Attacks against Small and Medium-sized Enterprises"* (Huaman et al. 2021b) analysiert, wie Unternehmensvertreter und -vertreterinnen das Risiko von Cyber-Angriffen wahrnehmen, wie verbreitet bestimmte Sicherheitsmaßnahmen sind, wie häufig verschiedene Typen von Cyber-Angriffen auf Unternehmen auftreten und schließlich, inwiefern sich bestimmte Unternehmensmerkmale und Sicherheitsmaßnahmen auf die Viktimisierung auswirken. Mit Blick auf das in Abbildung 2 dargestellte Referenzmodell geht der Beitrag auf die Variablen „Preventive Security", Reactive Security", „Compromise" und ansatzweise auf die Variable „Surface Exposure" ein.

Der **Beitrag C** *"Understanding the adoption of cyber insurance for residual risks - An empirical large-scale survey on organizational factors of the demand side"* (von Skarczinski et al. 2021) fokussiert das Thema „Cyber-Versicherung" als reaktive Sicherheitsmaßnahme und untersucht, wie weit verbreitet Cyber-Versicherungen in Unternehmen sind und was empirische Adaptionsfaktoren sind. Der Beitrag greift damit die Variablen „Preventive Security", „Surface Exposure" und „Compromise" auf, wobei „Compromise" als eine der unabhängigen Variablen in das Modell eingeht.

Der **Beitrag E** *"More Security, less Harm? Exploring the Link between Security Measures and Direct Costs of Cyber Incidents within Firms using PLS-PM"* (von Skarczinski et al. 2022a) untersucht, wie sich die direkten Kosten eines Cyber-Vorfalls im Hinblick auf bestehende Unternehmensmerkmale und implementierte Sicherheitsmaßnahmen erklären lassen. Bis auf die Variable „Threat", die durch die Datenerhebung nicht explizit gemessen wurde, werden in diesem Beitrag im Rahmen eines komplexen Zusammenhangmodells alle Bestandteile des oben dargestellten Referenzmodells aufgegriffen. Diese Abdeckung der Variablen des Referenzmodells erreichte bisher keine der von Woods und Böhme (2021) identifizierten Cyber-Risiko-Studien, weshalb sie die vollständige Abdeckung des Referenzmodells auch als "holy-grail-research" bezeichnen.
Der **Beitrag D** *"Toward enhancing the information base on costs of cyber incidents: implications from literature and a large-scale survey conducted in Germany"* (von Skarczinski et al. 2022b) verlässt die Ebene der Systematisierung von Cyber-Risiken und fokussiert sich auf deren deskriptive Quantifizierung. Untersucht werden die Forschungsfragen, welche Cyber-Angriffsarten Unternehmen als am schwerwiegendsten einschätzen und wie hoch die Kosten durch den schwerwiegendsten Angriff der letzten 12 Monate waren. Zudem stellt der Beitrag dar, was im Sinne eines Aktivitätenplans aus Perspektive von Unternehmen, Staat und Wissenschaft unternommen werden müsste, um zukünftig besser informierte Entscheidungen im Informationssicherheitsmanagement treffen zu können.
Der **Beitrag F** *"Modelling maximum cyber incident losses of German organisations: an empirical study and modified extreme value distribution approach"* (von Skarczinski et al. 2023) analysiert, wie mittels (modifizierter) Extremwertverteilungen die direkten Kosten von Cyber-Angriffen am besten modelliert werden können, welche unterschiedlichen Verteilungen mit Blick auf verschiedene Unternehmensmerkmale und Angriffsarten bestehen und welche Kosten auf Basis der modifizierten Extremwertverteilung für ein einzelnes Unternehmen und die deutsche Wirtschaft abgeleitet werden können. Damit ist dieser Beitrag im Bereich der probabilistischen Quantifizierung von Cyber-Risiken zu verorten.

2.4 Spektrum der angewandten Methoden und Theorien

Um die Forschungsfragen der Beiträge zu beantworten, wird auf verschiedene wissenschaftliche Methoden und Theorien zurückgegriffen. Der Hauptforschungsfrage der vorliegenden Dissertation folgend, inwiefern Cyber-Risiken erklärt und quantifiziert werden können, werden vor allem quantitative Methoden der Sozial- und Verhaltenswissenschaften angewendet, die einen wichtigen Anteil der Forschung in der Disziplin „information system research" ausmachen (Straub und Gefen 2004). Aus Perspektive der Erkenntnistheorie können die angewandten Methoden als positivistisch angesehen werden, weil im Allgemeinen davon ausgegangen wird, dass die Realität objektiv gegeben ist und durch messbare Eigenschaften beschrieben werden kann, die unabhängig vom Forscher und seinen Instrumenten sind (Myers 1997; Straub und Gefen 2004). So klassifizierten Orlikowski und Baroudi „information system research" als positivistisch, wenn es unter anderem Anzeichen für quantifizierbare Messungen von Variablen, Hypothesentests und das Ziehen von Schlussfolgerungen über ein Phänomen aus der Stichprobe auf eine bestimmte Population gab (Orlikowski und Baroudi 1991; Myers 1997).

Der Großteil der in den Forschungsbeiträgen angewandten Methoden folgt diesem positivistischen Paradigma, insofern quantitative Umfragedaten mithilfe quantitativer Analysemethoden ausgewertet werden, um die Ergebnisse zu diskutieren und aus ihnen Schlussfolgerungen bzw. Handlungsempfehlungen abzuleiten. Der Datensatz des KFN-Forschungsprojektes „Cyberangriffe gegen Unternehmen“ umfasst die Angaben der quantitativen Computer-Assissted-Telephone-Interviews mit 5.000 Deutschen Unternehmensvertretern sowie die in den Unternehmensdatenbanken Bisnode und Heins&Partner enthaltenen Stammdaten der Unternehmen (z.B. Branchenzugehörigkeit, Sitz, Umsatz, etc.), wodurch ein in Umfang und Detailtiefe weltweit nahezu einzigartiger Datensatz entstanden ist (siehe Literaturrecherche in Dreißigacker et al. 2020b). Die Repräsentativität, gerade auch mit Blick auf kleine und mittelständische Unternehmen, und die Kontrolle über die Zufallsziehung (im Sinne der Stratifikation und Ausfall- und Abbruchanalyse) sind Qualitätsmerkmale, die wenige der bisherigen empirischen Cyber-Risiko-Studien teilen (vgl. von Skarczinski et al. 2023; von Skarczinski et al. 2022a; von Skarczinski et al. 2022b). Diese basieren demgegenüber überwiegend[9] auf sehr kleinen Stichproben mit wenig Differenzierungsmöglichkeiten (z.B. Paoli et al. 2018; Herath et al. 2020), aus Daten einzelner Organisationen (z.B. Kuypers et al. 2016; Pate-Cornell und Kuypers 2021) oder aus Daten öffentlicher bzw. kommerzieller „OpRisk“-Datenbanken (z.B. Romanosky 2016; Biener et al. 2015; Strupczewski 2019; Eling und Wirfs 2019; Jung 2021; Edwards et al. 2016; Aldasoro et al. 2020), für die die Repräsentativität und Vollständigkeit der Datensätze nicht sichergestellt werden können.[10] Die Schwächen solcher öffentlicher bzw. kommerzieller Datenbasen können hingegen durch repräsentative Befragungen ausgeglichen werden (Wheatley et al. 2021), die auch die Basis der Forschungsbeiträge A bis F sind (siehe Tab. 2).

Auch der in Forschungsbeitrag A verwendete Datensatz der Landeskriminalämter Niedersachsen und Schleswig-Holstein zur Kriminalitätsbefragung der Bevölkerung weist aufgrund seiner kontrollierten Stichprobenziehung (Zufallsstichprobe auf Basis von Daten der Einwohnermeldeämter sowie postalischer Versand des Fragebogens) und dem großen Stichprobenumfang (N=33.538) eine hohe Repräsentativität auf.

[9] Es existieren einige wenige repräsentative Surveys zu Cyber Risiken, z.B. Rantala 2008, Richards 2009 und DCMS 2022, die sich jedoch vorwiegend auf die deskriptive Beschreibung der Deliktsentwicklung fokussieren.

[10] So enthält z.B. die von Strupczewski 2019 und Eling 2019 genutzte SAS OpRisk Database nur Verlust-Ereignisse, die öffentlich berichtet wurden und 100.000 USD übersteigen, womit kleinere Schäden oder auch Vorfälle von kleinen und mittelständischen Unternehmen unberücksichtigt bzw. stark unterrepräsentiert sind (vgl. auch Wolff und Lehr 2017).

Beitrag	Methode / Datenbasis	Theorie / Modell	Ergebnis / Output
A	✓ Literatur-Review[11] ✓ Deskriptive Statistik ✓ Regressionsmodelle, binär logistisch ✓ Datensatz der LKA-Kriminalitätsbefragung SH und NDS (N=33,538)	✓ Routine Activity Approach (Cohen und Felson 1979)	✓ Risikofaktoren von Cyber-dependent Crime für verschiedene Deliktarten
B	✓ Literatur-Review ✓ Deskriptive Statistik ✓ Regressionsmodelle, linear und logistisch ✓ Datensätze des KFN-Forschungsprojektes (N=5,000)	✓ Explorativ, Modellselektion nach AIC (Akaike Information Criterion, Akaike 1974)	✓ Erklärende Faktoren für ✓ Risikobewusstsein ✓ Adaption von Sicherheitsmaßnahmen ✓ Gemeldete Cyber-Angriffe ✓ Handlungsempfehlungen
C	✓ Literatur-Review ✓ Deskriptive Statistik ✓ Regressionsmodelle, binär logistisch ✓ Datensätze des KFN-Forschungsprojektes (N=5,000)	✓ TOE-Framework (DePietro et al. 1990)	✓ Adaptionsfaktoren von Cyber-Versicherungen ✓ Handlungsempfehlungen
D	✓ Literatur-Review (Webster und Watson 2002) ✓ Deskriptive Statistik ✓ Experten-Interviews ✓ Datensätze des KFN-Forschungsprojektes (N=5,000)	keine	✓ Strukturierte Literaturmatrix ✓ Cyber-Kosten Benchmark ✓ Aktivitätsplan, um Informationsbasis zu Cyber-Kosten zu verbessern
E	✓ Literatur-Review ✓ Deskriptive Statistik ✓ Strukturgleichungsmodelle, Partial Least Squares ✓ Datensätze des KFN-Forschungsprojektes (N=5,000)	✓ IS Cause-and-Effect-Model of Cohen et al. (1998) ✓ Cyber-Risk Model of Woods und Böhme (2021)	✓ Empirisches Kausalmodell zu Schäden durch Cyber-Angriffe
F	✓ Literatur-Review ✓ Deskriptive Statistik ✓ Stochastische Modellierung ✓ Datensätze des KFN-Forschungsprojektes (N=5,000)	✓ Extreme Value Theory (Coles 2001; Beirlant et al. 2004)	✓ Modifizierter Ansatz für Extremwertverteilungen ✓ Verteilungsmodelle / Parameter für Verluste durch Cyber-Angriffe nach verschiedenen Merkmalen ✓ Hochrechnung für nationale Cyber-Verluste
Relevante Vorarbeiten im KFN-Forschungs-projekt	✓ Literatur-Review (Webster und Watson 2002) ✓ Experten-Interviews ✓ Qualitative Inhaltsanalyse (Mayring 2014)	keine	✓ CATI-Fragenbogen ✓ Online-Fragebogen ✓ Datenerhebung

Tab. 2: In den Forschungsbeiträgen angewandte Methoden und Theorien/Modelle.

[11] Der Forschungsstand wurde aus Gründen von Seitenanzahlrestriktionen nicht im Beitrag A abgedruckt. Eine deutschsprachige, leicht erweiterte Version des Beitrages inklusive des Forschungsstandes wurde jedoch im Springer VS Verlag veröffentlicht (vgl. Dreißigacker et al. 2020a.)

In Tabelle 2 werden die in den Forschungsbeiträgen angewandten Methoden und Theorien bzw. Modelle dargestellt. Nach einem Literatur-Review, der zu jedem Beitrag den Stand der aktuellen Forschung dargestellt (vgl. Fettke 2006), wurden einer Theorie bzw. einem Modell folgend deskriptive, inferenzstatistische oder stochastische Analysen durchgeführt. Beitrag D, als Ausnahme, unterliegt keiner Theorie bzw. keinem Modell, da die wesentlichen Ziele des Beitrages die Literaturübersicht, die Bereitstellung von Benchmark-Daten sowie die Aufstellung eines Aktivitätenplanes sind. In der letzten Spalte der Tabelle 2 werden die Kernergebnisse in Form von konkreten Outputs bzw. Liefergegenständen überblickartig aufgeführt und im folgenden Abschnitt detaillierter beschrieben.

3 Zusammenfassung der Forschungsergebnisse

Für die zusammenfassende Darstellung der zentralen Forschungsergebnisse aus den Beiträgen A bis F wird das Phänomen Cyber-Risiken bzw. Cyber-Angriffe zunächst mit Blick auf die Verbreitung und Häufigkeit eingeordnet, um anschließend empirische Risiko- und Schutzfaktoren aufzuzeigen (vgl. Teilbereich 1 in Abb. 2). In einem weiteren Schritt wird auf die deskriptive und stochastische Quantifizierung des Cyber-Risikos eingegangen (vgl. Teilbereich 2 in Abb. 2). Die detaillierten Ergebnisse sowie weitere Verweise auf einschlägige Literatur wurden in den jeweiligen Forschungsbeiträgen veröffentlicht.

3.1 Dimensionierung des Phänomens

Cyber-Risiken und Cyber-Angriffe sind allgegenwärtig, jedoch werden Verbreitung und Ausmaß des Phänomens immer wieder kontrovers diskutiert. So wird beispielsweise kommerziellen Studien vorgeworfen, Verluste aus Cyber-Vorfällen aus diversen Gründen zu überschätzen (Wolff und Lehr 2017; Paoli et al. 2018; Anderson et al. 2019). Polizeiliche Kriminalstatistiken leiden hingegen darunter, dass viele Vorfälle nicht angezeigt und statistisch erfasst werden (sog. relatives Dunkelfeld) bzw. dass Organisationen gar nicht erst bemerken, dass sie Opfer eines Cyber-Angriffs wurden (sog. doppeltes oder absolutes Dunkelfeld) (Buil-Gil et al. 2021; Dreißigacker et al. 2020b). Daher sind wissenschaftliche Studien umso wichtiger, um das Ausmaß von Cyber-Risiken und das Ausmaß des relativen Dunkelfeldes zu ergründen.

Nicht nur Organisationen, sondern auch Individuen sind durch Cyber-Angriffe betroffen. Auf Basis einer repräsentativen Viktimisierungsbefragung der Bevölkerung in Schleswig-Holstein und Niedersachsen aus dem Jahre 2015 (N=33,538) zeigt sich, dass ein erheblicher Anteil der befragten Bevölkerung (16,6 %) von mindestens einer Viktimisierung durch Cyber-Kriminalität im engeren Sinne während des Jahres 2014 betroffen war (Bergmann et al. 2018). Die Malware-Infektion war die häufigste Form der Viktimisierung (11,5 %). Ransomware-Infektionen und Missbrauch von persönlichen Daten wurden seltener festgestellt (3,6 % bzw. 5,3 %). Auch wenn aufgrund der unterschiedlichen Kriminalitätsformen die Prävalenzraten zwischen Individuen und Organisationen nicht direkt vergleichbar sind, zeigt sich mit Blick auf die CATI-Befragung von 5.000 deutschen Unternehmen mit mehr als neun Mitarbeitenden eine deutlich höhere Betroffenheit. Die teilnehmenden Unternehmen schätzen ihre Risiken durch gezielte bzw. massenhafte Cyber-Angriffe zwar (eher) gering ein (vgl. Abb. 3), jedoch gaben 45,1 % an, dass ihr Unternehmen in den letzten 12 Monaten aktiv auf mindestens einen Vorfall reagieren musste. Bei mehr als der Hälfte von ihnen geschah dies mehrfach in diesem Zeitraum. Abbildung 4 veranschaulicht die gemeldeten Vorfälle, die nicht immer gleichermäßig auf die Branchen verteilt sind.

Ein wichtiger Aspekt in der Dimensionierung des Phänomens ist nicht nur die Frage, ob eine Viktimisierung eintrat oder nicht, sondern auch inwiefern dadurch

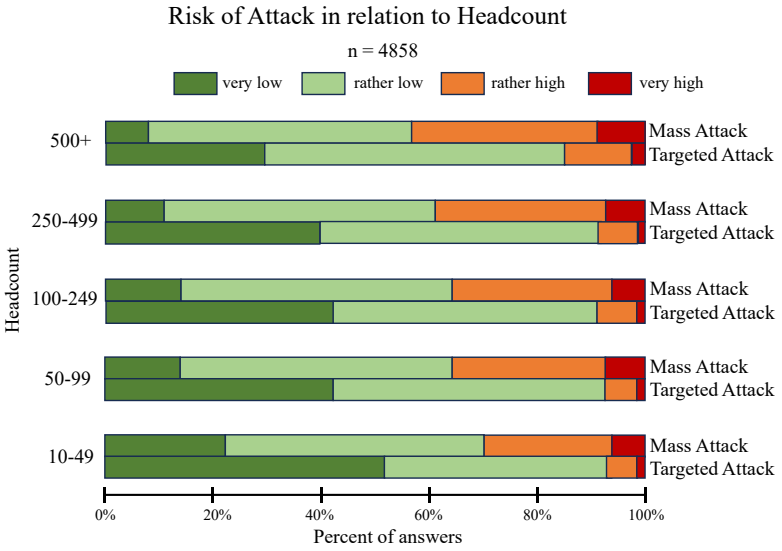

Abb. 3. Risikoeinschätzung nach massenhaften bzw. gezielten Angriffen und Beschäftigtengrößenklasse (Huaman et al. 2021b).

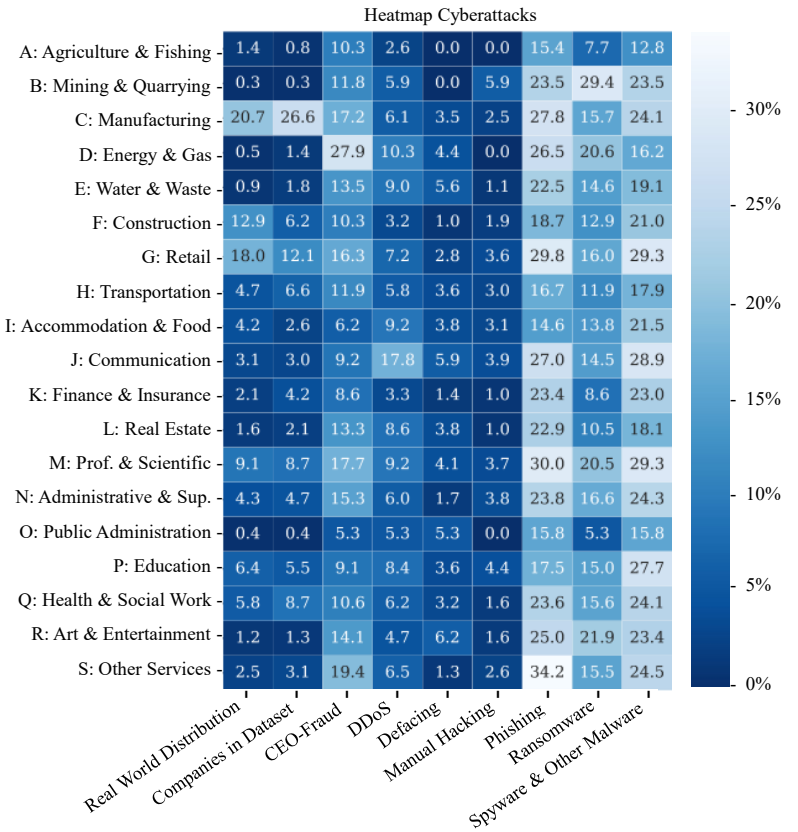

Abb. 4: Heatmap mit Prozentsatz der Unternehmen je Branche, die in den letzten 12 Monaten aktiv auf mindestens einen Angriff reagieren mussten (Huaman et al. 2021b).

Schäden entstanden sind. Die Bezifferung dieser Schäden durch Cyber-Angriffe ist aus mehreren Gründen schwierig. Nicht alle Unternehmen bemerken Schäden, wollen oder können diese ermitteln oder, sofern Schäden ermittelt wurden, wollen diese offenlegen. Mit Blick auf die Beschäftigtengrößenklassen zeigt sich, dass gerade kleinere Unternehmen weniger häufig über einen schwerwiegenden Vorfall berichteten und hingegen größere Unternehmen öfter über Schadensschätzungen in Euro-Werten Auskunft gaben (vgl. Abb. 5).

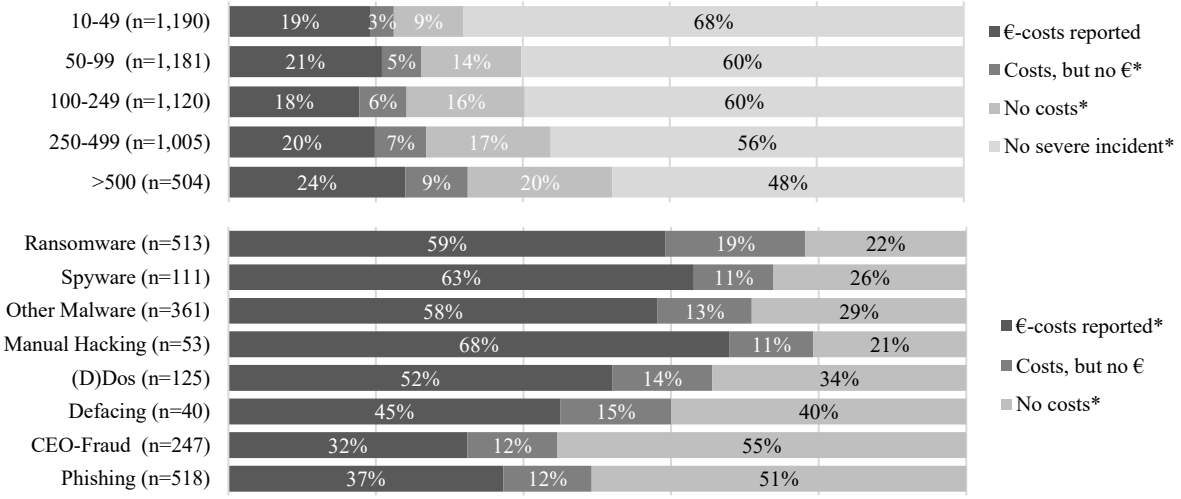

Abb. 5: Anteil der Unternehmen nach Beschäftigtengrößenklasse und Angriffsart, die Kosten ihres schwerwiegendsten Vorfalls der letzten 12 Monate berichteten (von Skarczinski et al. 2022b).

Wenn größere Unternehmen von ihrem schwerwiegendsten Vorfall berichteten, lagen deutlich häufiger Angaben zu finanziellen Schäden vor, wobei es auch hier Unterschiede zwischen den verschiedenen Angriffsarten gab (vgl. Abb. 5). Insgesamt berichteten rund zwei Fünftel der Unternehmen der repräsentativen Stichprobe (N=5,000) von einem schwerwiegendsten Angriff in den letzten 12 Monaten, wovon ca. die Hälfte Angaben zu geschätzten Schäden machte. Dies bedeutet, dass ein wesentlicher Anteil der Unternehmen Schäden durch Cyber-Angriffe erlitt, womit sich die Frage stellt, von welchen Eigenschaften das Cyber-Risiko abhängt.

3.2 Einflussfaktoren von Cyber-Risiken

Nachfolgend werden die Erkenntnisse aus den Forschungsbeiträgen A bis F zusammengefasst, die auf empirischer Basis untersuchten, welche Faktoren Cyber-Risiken begünstigen bzw. mindern oder die Adaption von Sicherheitsmaßnahmen beeinflussen.

3.2.1 Risikofaktoren

Faktoren, die das Cyber-Risiko beeinflussen, können technologischen, organisatorischen/prozessualen oder behavioristischen Ursprüngen zugeordnet werden (Woods und Böhme 2021). Auf letztere, die behavioristischen und kontextrelevanten Merkmale von Individuen, die Opfer von Cyber-Angriffen werden, fokussiert sich Forschungsbeitrag A (Bergmann et al. 2018). Die binär logistischen Regressionsmodelle zeigen u.a., dass das männliche

Geschlecht häufiger in Verbindung mit Malware- (AME: -0,021)[12] und Ransomware-Infektionen (AME: -0,032) steht, während die Variable „Alter“ keine relevanten Effekte auf eine Viktimisierung hat. Individuen in einer besseren ökonomischen Situation zeigen für alle drei berücksichtigten Angriffsarten (Malware, Ransomware, Missbrauch personenbezogener Daten) ein geringeres Viktimisierungsrisiko. Ein höheres Bildungslevel zeigt keinen Effekt auf Malware- und Ransomware-Infektionen, erhöht jedoch das Risiko des Missbrauchs personenbezogener Daten um durchschnittlich 2,9%. Zudem hebt eine höhere Internetnutzung durch Individuen das Risiko für Malware-Infektionen um durchschnittlich 2,3%. Sowohl schützende als auch vermeidende Verhaltensweisen haben eine risikomindernde Wirkung auf die Wahrscheinlichkeit, von Cyber-Vorfällen betroffen zu sein. Allerdings hatte das Schutzverhalten auch einen positiven Effekt auf das Risiko des Missbrauchs personenbezogener Daten, was mit Blick auf den Routine-Activity-Ansatz als theoretische Basis nicht den Erwartungen entsprach. Darüber hinaus zeigen die multivariaten Ergebnisse, dass individuelle Faktoren und Haushaltsfaktoren sowie das Online- und Präventionsverhalten das Risiko der Viktimisierung beeinflussen. Dies bedeutet, dass das Risiko einer Viktimisierung nicht für alle Individuen gleich ist. Insgesamt stehen die Ergebnisse im Einklang mit dem Routine-Aktivitäts-Ansatz: Das Vorhandensein von Cyber-Vorfällen hängt neben anderen Faktoren vom routinemäßigen (Online-)Verhalten der Nutzer und Nutzerinnen und dem Fehlen von fähigen Wächtern (dem Vorhandensein von Präventionsfaktoren) ab.

Mit Forschungsbeitrag B (Huaman et al. 2021b) wechselt nun die Perspektive von dem Individuum auf das Unternehmen und die wahrgenommenen Vorfälle der letzten 12 Monate. Die binär logistischen Regressionsanalysen zeigen vor allem, dass der Einfluss von Risiko- und Schutzfaktoren auf die Viktimisierung zwischen den Unternehmensbranchen und Angriffsarten variieren. So wurden beispielsweise (Distributed)-Denial-of-Service-Angriffe (DDoS) vermehrt aus der Kommunikationsbranche berichtet, wohingegen Phishing durch die Zugehörigkeit zur Branche Handel sowie CEO-Fraud durch die Branchen Energie und sonstige Dienstleistungen beeinflusst wurde (vgl. auch Tab. 3).

CEO-Fraud	O.R.	C.I.	p-value
Interviewee Position			
Tech	**1.42**	**[1.09, 1.85]**	**<0.01***
Information Security Policies or Incident Response Plan	**1.68**	**[1.14, 2.47]**	**<0.01***
Information Security Certification	1.01	[0.81, 1.27]	0.91
Information Security Policy Enforcement	0.95	[0.73, 1.24]	0.71
Risk Analysis	1.15	[0.93, 1.43]	0.20
Company Age	1.10	[0.66, 1.84]	0.71
Export Activity	1.11	[0.87, 1.42]	0.40
Multiple National Branches	**1.29**	**[1.06, 1.58]**	**0.01***
International Branches	**1.52**	**[1.17, 1.97]**	**<0.01***
Industry Sector (only levels with significance displayed)			
D: Energy & Gas	**2.34**	**[1.02, 5.34]**	**0.04***
S: Other Services	**2.34**	**[1.18, 4.63]**	**0.01***
Per 1 Mio Annual Turnover	**1.00**	**[1.00, 1.00]**	**<0.01***
Employees Tech (Per 100)	1.00	[1.00, 1.00]	0.27
Employees (Per 100)	**1.20**	**[1.12, 1.28]**	**<0.01***

Tab. 3: Ergebnisse der logistischen Regression für CEO-Fraud Vorfälle (O.R.: Odds Ratio; C.I. Konfidenzintervall α=5; Huaman et al. 2021b)

Unternehmensmerkmale wie die internationale Geschäftstätigkeit und Unternehmensgröße stehen in Zusammenhang mit dem häufigeren Bericht von Cyber-Vorfällen. Dies gilt auch für Unternehmen mit mehreren Standorten. Die Regressionsergebnisse zeigten auch, dass organisatorische Maßnahmen (z.B. das Vorhandensein von IS-Richtlinien und Notfallplänen) häufiger mit der Meldung von Sicherheitsvorfällen in Zusammenhang stehen als die implementierten technischen Sicherheitsmaßnahmen. Dagegen wiesen Unternehmen, die häufiger technische Sicherheitsmaßnahmen einsetzten, nicht mehr Sicherheitsvorfälle auf.

[12] Average Marginal Effects (AME); AMEs lassen sich als durchschnittliche prozentuale Veränderung der Wahrscheinlichkeit eines abhängigen Zustands interpretieren, wenn sich die unabhängige Variable um eine Einheit verändert. Beispiel: Die Wahrscheinlichkeit Opfer eines Malware-Angriffes zu werden, ist für Frauen im Durchschnitt 2,1% geringer als für Männer

Allerdings korrelierte die Meldung von organisatorischen Maßnahmen mit der Meldung bestimmter Arten von Vorfällen (z.B. Ransomware, CEO-Fraud).
Nach den zusammengefassten Ergebnissen der Regressionsanalysen aus den Forschungsbeiträgen A und B, welche jeweils den Einfluss verschiedener unabhängiger Variablen auf eine abhängige Variable untersuchen, fokussiert sich Forschungsbeitrag E (von Skarczinski et al. 2022a) auf die Erstellung und Validierung eines Strukturgleichungsmodells (Partial Least Squares Path Modelling; PLS-PM), welches die Beziehung verschiedener latenter und emergenter Variablen analysiert (Abb. 6). Im Mittelpunkt stehen die von den Unternehmen berichteten schwerwiegendsten Cyber-Angriffe der letzten 12 Monate, die technische und finanzielle Schäden zur Folge hatten.

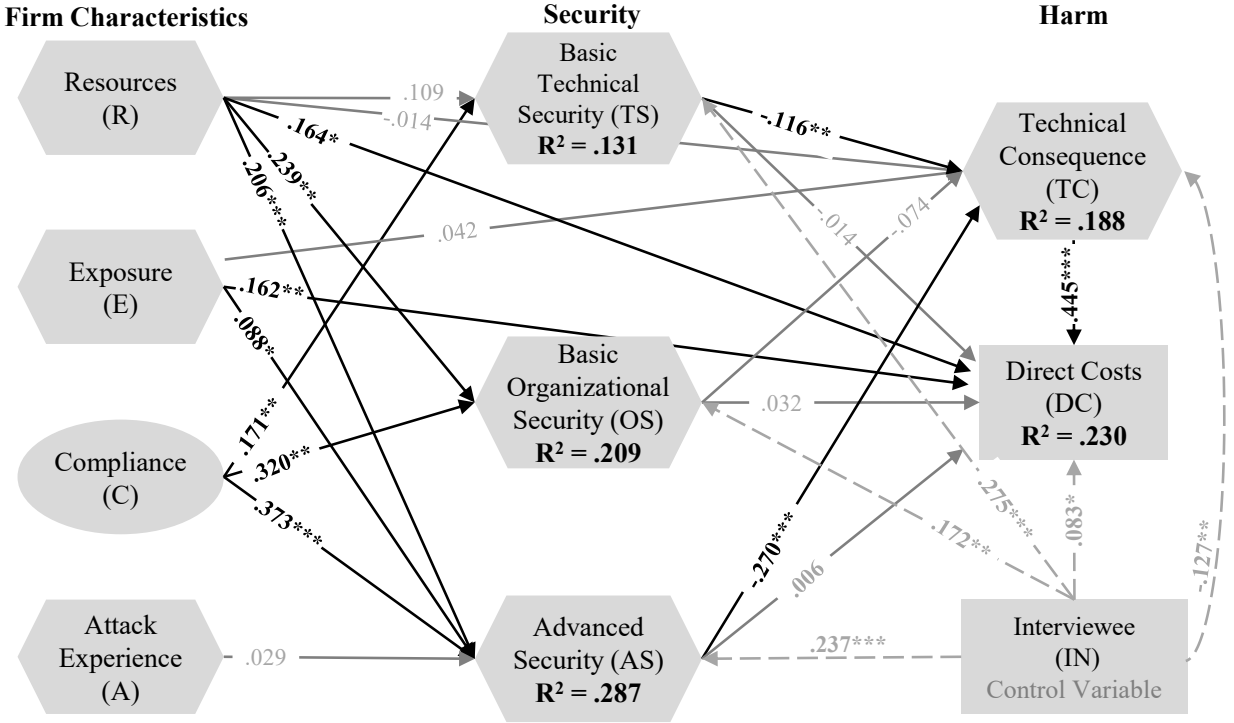

Abb. 6: PLS-Strukturgleichungsmodell (N=493; *p < .05, **p < .01, ***p < .001; von Skarczinski et al. 2022a)

Das Modell zeigt, dass ein erhöhtes „Exposure“, bestehend aus den Indikatoren Export-Aktivität, Anzahl der Lokationen in Deutschland und im Ausland, die Bereitstellung besonderer Produkte/Services oder eine besondere Reputation oder Kundenbasis einen unmittelbaren Einfluss auf die direkten Kosten des schwerwiegendsten Angriffs der letzten 12 Monate hat. Im Modell bestehen die „Direct Costs“ aus der logarithmierten Summe (EUR) von sechs zugrundeliegenden Kostenpositionen, die entweder direkte Kosten oder Opportunitätskosten sind (1. Kosten für externe Beratung & Unterstützung; 2. Buß- und Entschädigungsgelder; 3. Abfluss von finanziellen Mitteln; 4. Kosten für Ersatz & Wiederherstellung; 5. Verteidigungs- und Ermittlungskosten / Personalkosten; 6. Umsatzverluste / Betriebsunterbrechung), die von den Befragten geschätzt wurden. Die Koeffizienten können interpretiert werden als die Veränderung des abhängigen Konstrukts gemessen in Standardabweichungen, wenn ein unabhängiges Konstrukt um eine Standardabweichung erhöht wird, während alle anderen erklärenden Konstrukte konstant bleiben (Benitez et al. 2020). Demnach erhöhen sich die „direct Costs“ um 0,162 Standardabweichungen, wenn das „Exposure“ um eine Standardabweichung ansteigt. Auf die „Technical Consequences“, gemessen in der logarithmierten Ausfallzeit von Systemen in Stunden sowie die Anzahl der

ausgefallenen Systeme, zeigte sich zwar kein signifikanter Einfluss von „Exposure“. Jedoch erhöhten mehr „Resources“ in Form von mehr Mitarbeitenden, mehr IT-Sicherheitsmitarbeitenden und einem höheren IT-Sicherheitsbudget die direkten Kosten des schwerwiegendsten Vorfalls, da mit mehr Ressourcen auch größere Unternehmen mit mehr Umsatz, Vermögensgegenständen, Systemen und prozessualen bzw. technischen Vernetzungen einhergehen. Neben Unternehmensmerkmalen, die sich risikosteigernd auswirken, wurden auch Schutz- und Adaptionsfaktoren untersucht.

3.2.2 Schutz- und Adaptionsfaktoren

Das PLS-Strukturgleichungsmodell (Abb. 6) weist darauf hin, dass das Vorhandensein von grundlegenden technischen Sicherheitsmaßnahmen, wie Mindestanforderungen für Passwörter, die Vergabe individueller Nutzerrechte, regelmäßige Datensicherungen, der Einsatz von Firewalls und Antiviren-Software die technischen Konsequenzen eines Cyber-Angriffes direkt beeinflusst. Analog ist dies auch für erweiterte Sicherheitsmaßnahmen „Advanced Security“ der Fall, welche sich aus den Faktoren Sicherheitszertifizierung, regelmäßige Risiko-Assessment/Penetrationstests, Ausfallsimulationen und den Einsatz von NextGen Firewalls zusammensetzen. Organisatorische Basismaßnahmen haben im Modell keinen signifikanten Einfluss auf die technischen Konsequenzen. Insgesamt zeigen die drei emergenten Sicherheitsvariablen keinen unmittelbaren Einfluss auf die direkten Kosten. Jedoch stehen grundlegende technische und erweiterte Sicherheitsmaßnahmen im direkten Zusammenhang mit den technischen Konsequenzen, die wiederrum einen starken Einfluss auf die „Direct Costs“ aufweisen. Mit Blick auf die Frage, welche Faktoren in einer Organisation im Zusammenhang mit der Implementierung von grundlegenden und erweiterten Sicherheitsmaßnahmen stehen, wird deutlich, dass die latente Variable „Compliance“, operationalisiert durch die Faktoren Risiko/Compliance-Einschätzung von Geschäftsführenden und Belegschaft sowie die Einschätzung der allgemeinen Security-Bemühungen, einen wichtigen Einfluss hat. Die Erkenntnisse aus dem PLS-Strukturgleichungsmodell (Abb. 7) können dahingehend vereinfacht zusammengefasst werden, als dass die Sensibilisierung der Geschäftsführung und der Belegschaft sich positiv auf das Vorhandensein grundlegender und erweiterter Sicherheitsmaßnahmen auswirkt, technische und erweiterte Sicherheitsmaßnahmen die technischen Konsequenzen des schwerwiegendsten Angriffs mindern, die dann wiederum mit geringeren direkten Kosten verbunden sind. Parallel dazu werden die direkten Kosten eines Angriffes durch eine höhere Angriffsfläche und Größe der Organisation beeinflusst.

Mit Blick auf alle erlebten Cyber-Angriffe der befragten Unternehmen in den letzten 12 Monaten zeigt Forschungsbeitrag B auf, dass nur wenige einzelne Sicherheitsmaßnahmen einen direkten mindernden Einfluss auf die Betroffenheit haben und sich zudem zwischen den Angriffsarten unterscheiden. So steht das Vorhandensein von Informationssicherheitsrichtlinien und Notfallplänen im Zusammenhang mit mehr berichteten Vorfällen von Ransomware, CEO-Fraud, Defacing und Phishing. Mutmaßlich stehen diese Maßnahmen eher für eine höhere Reife der Informationssicherheit, die dazu führt, dass mehr Angriffe entdeckt und behandelt werden. Im Gegensatz dazu scheint die Durchsetzung von Informationssicherheitsrichtlinien für alle Angriffsarten, mit Ausnahme von (D)DoS-Angriffen, einen Einfluss auf eine geringe Betroffenheit zu haben.

Eine weitere Sicherheitsmaßnahme, die nicht primär auf die Vermeidung von Cyber-Vorfällen abzielt, sondern die Schäden daraus mindern soll, sind Cyber-Versicherungen (CV). Cyber-Versicherungen wurden als wachsendes Phänomen gesehen, um Residualrisiken zu mitigieren (Dambra et al. 2020; Kshetri 2020; Marotta et al. 2017), jedoch wurde der tatsächliche Beitrag zum Informationssicherheitsmanagement aus verschiedenen Gründen immer wieder kritisch diskutiert (Bandyopadhyay et al. 2009; Böhme et al. 2010; Branley-Bell et al. 2022). Forschungsbeitrag C (von Skarczinski et al. 2021) untersucht auf Basis des TOE-Frameworks (DePietro et al. 1990) die Fragestellung, welche technischen, organisatorischen und umweltbedingten Adaptionsfaktoren das Vorhandensein von Cyber-Versicherungen (CV) beeinflussen. Auf Basis der repräsentativen Stichprobe gaben rund 19,5% der Unternehmen an, eine Versicherung abgeschlossen zu haben, die Auswirkungen durch Cyber-Angriffe abdeckt. Die Adaptionsraten unterscheiden sich jedoch nach Branche und Unternehmensgröße insofern, dass vor allem Unternehmen mit mehr als 500 Mitarbeitenden und Unternehmen der Branche „Finanzen“ CV abschlossen (vgl. Abb. 7). Weitere 20,3% der Unternehmen haben einen Abschluss geprüft, aber nicht vollzogen.

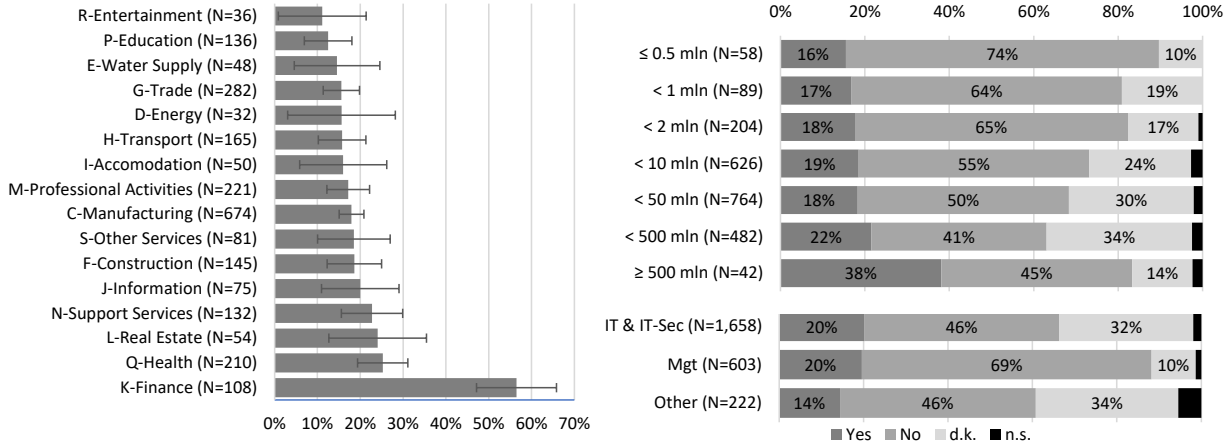

Abb. 7: Adaption von Cyber-Versicherungen in Prozent nach WZ08-Klassifikation, nach Umsatzklasse in Mio. EUR und nach Position der befragten Person (Konfidenzintervall α=5%; d.k.: do not know; n.s.: not specified; von Skarczinski et al. 2021).

Mit Blick auf die Unternehmenskomplexität wird deutlich, dass Unternehmen mit mehreren Standorten und eigener IT-Infrastruktur in Deutschland signifikant häufiger zu CV neigen (AME: 0,074). Die Auslagerung von Software oder Speicherplatz in eine externe Cloud hat ebenfalls einen positiven Effekt (AME: 0,074), wohingegen die Auslagerung von E-Mail/anderen Kommunikationssystemen negativ mit dem Einsatz von CV zusammenhängt (AME: -0,077). Unternehmen mit Notfallrichtlinien weisen jedoch eine signifikant erhöhte Wahrscheinlichkeit von 16% (AME: 0,159) auf auch Versicherungsschutz zu besitzen. Hinsichtlich der Ressourcen ist kein signifikanter Zusammenhang zwischen IT oder IT-Sicherheitspersonal/Budget und der Entscheidung für oder gegen CV festzustellen. Erfahrungen mit verschiedenen Arten von Cyber-Angriffen in den letzten 12 Monaten zeigen keine signifikante Korrelation mit der Einführung von CV, mit Ausnahme von CEO-Betrug (AME: -0,114). Dies bedeutet, dass Unternehmen, die einen solchen Angriff erlebt haben, mit geringerer Wahrscheinlichkeit über CV verfügen. Auch die erhöhte Risikowahrnehmung von Unternehmensvertretern und Unternehmensvertreterinnen kann weder positiv noch negativ mit der Einführung von CV in Verbindung gebracht werden. Zwar konnten TOE-relevante Adaptionsfaktoren empirisch nachgewiesen werden, jedoch blieb ein

Großteil der TOE-basierten Hypothesen zur Adaption von CV unbestätigt.

3.3 Quantifizierung

Wie in Abbildung 2 dargestellt, können Cyber-Risiken mithilfe verschiedener Methoden quantifiziert werden. Forschungsbeitrag D (von Skarczinski et al. 2022b) fokussiert sich auf eine deskriptive Analyse der durch den schwerwiegendsten Cyber-Angriff entstandenen Kosten und bietet Unternehmen und Forschenden eine strukturierte und niedrigschwellige Grundlage um 1.) eigene Cyber-Risiko-Quantifizierungen auf Basis der Erkenntnisse zu ermitteln oder 2.) eigene Cyber-Risiko-Quantifizierungen mit den empirischen Daten zu vergleichen (Benchmarking). Forschungsbeitrag F hingegen ist stochastischer Natur und modelliert mittels (modifizierter) Extremwertverteilungen die direkten Kosten von Cyber-Angriffen. Der Beitrag bietet Forschenden und Experten und Expertinnen mit Cyber-Risiko-Fachwissen geeignete Wahrscheinlichkeitsverteilungen, um eigene stochastische Cyber-Risiko-Modelle erstellen oder validieren zu können. Beide Beiträge unterscheiden verschiedene Kosten- und Angriffsarten (vgl. Abb. 8) sowie fünf Beschäftigtengrößenklassen und die Branchenzugehörigkeit nach der WZ08-Klassifikation.

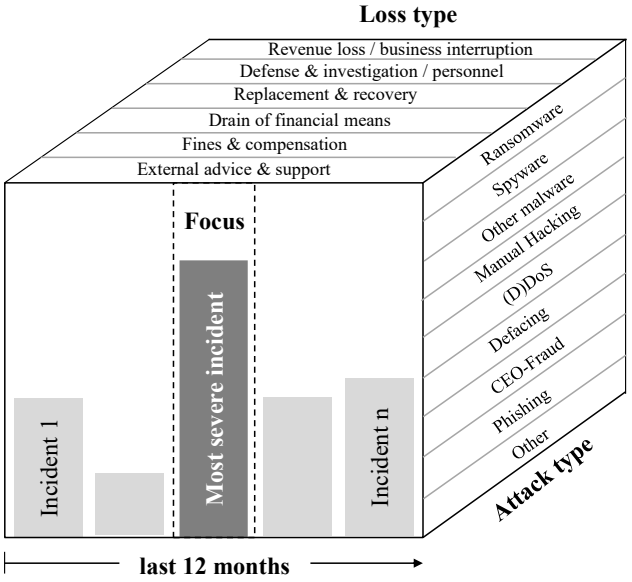

Abb. 8: Operationalisierung der Kosten von Cyber-Angriffen (von Skarczinski et al. 2023).

Fasst man die Erkenntnisse aus Forschungsbeitrag D zusammen, berichten nur zwei Fünftel der 5.000 Unternehmen, in den letzten 12 Monaten einen schweren Cyber-Vorfall erlebt zu haben. Von diesen zwei Fünfteln gibt jedes zweite Unternehmen an, dass keine Kosten entstanden sind und nur 3,1 % melden Kosten von mehr als 50.000 Euro (vgl. Abb. 9).

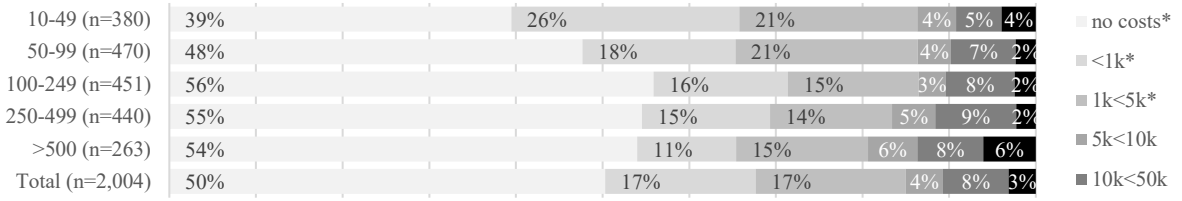

Abb. 9: Anteile (%) von klassifizierten Gesamtkosten in TEUR (Chi-Square: *p<.05; von Skarczinski et al. 2022b).

Die maximalen Kosten für einen Cyber-Angriff im Datensatz liegen bei 2 Millionen Euro. Jedoch unterscheiden sich die Kosten für einen Angriff je nach Angriffsart und Beschäftigtengrößenklasse (vgl. Tab. 4). Die Gesamtkosten liegen, ohne Berücksichtigung der Unternehmen, die zwar Schäden, aber keine geschätzten Kosten in Euro meldeten, bei 20.348 EUR im Durchschnitt und

1.400 EUR im Median. Abgesehen von sonstigen und kombinierten Angriffen, für die nur wenige Beobachtungen vorliegen, fallen vor allem manuelle Hacking-Angriffe, die auch die Manipulation von Hardware und unautorisierte Konfiguration beinhalten, auf. Dort liegen die berichteten Kosten bei rund 50.111 EUR im Durchschnitt und 2.900 EUR im Median. Von den 805 Fällen, in denen die teilnehmenden Unternehmen gültige Antworten zu allen Kostenpositionen gaben (secured total costs), waren mehr als ein Viertel Ransomware-Angriffe, die mit einem Median von 2.000 EUR vergleichsweise hohe Kosten verursacht haben.

		Secured total costs excl. zero costs					
		Total	**10-49**	**50-99**	**100-249**	**250-499**	**>500**
Ransom-ware	avg	19,380	30,646	7,566	15,935	25,246	12,737
	med	2,000	1,300	1,300	1,550	2,000	2,005
	n	*221*	*43*	*47*	*40*	*65*	*26*
Spyware	avg	6,347	10,728	5,440	3,480	2,535	3,040
	med	1,600	750	1575	3000	1650	1200
	n	62	21	18	10	8	5
Other Malware	avg	12,728	8,822	15,968	15,742	7,198	17,715
	med	1,000	750	1000	1750	1200	500
	n	*172*	*54*	*43*	*36*	*22*	*17*
Manual Hacking	avg	50,111	37,900	11,443	108,411	32,500	5,667
	med	2,900	2,800	2,000	2,000	32,500	5,000
	n	*28*	*7*	*7*	*9*	*2*	*3*
(D)DoS	avg	35,457	18,525	57,289	9,609	15,595	164,040
	med	1,500	1,100	2,000	1,000	4,003	1,200
	n	*55*	*18*	*9*	*13*	*10*	*5*
Defacing	avg	2,203	2,788	2,333	1,633	600	
	med	1,245	990	2000	500	600	
	n	*12*	*5*	*3*	*3*	*1*	
CEO-Fraud	avg	38,816	1,449	2,381	14,521	93,489	30,222
	med	1,000	500	500	750	1250	5500
	n	*68*	*7*	*15*	*12*	*22*	*12*
Phishing	avg	18,997	5,539	37,199	19,919	4,481	24,962
	med	1,100	1,000	1,800	1,000	1,000	1,750
	n	*172*	*35*	*46*	*30*	*37*	*24*
Other	avg	41,567	41,567				
	med	4,000	4,000				
	n	*3*	*3*				
Combined attacks	avg	8,592		3,500	1,150	27,000	
	med	1,500		3,000	1,000	2,000	
	n	*12*		*5*	*4*	*3*	
Total	avg	20,348	15,341	18,172	19,878	25,557	26,592
	med	1,400	1,000	1,300	1,500	1,650	2,000
	n	*805*	*193*	*193*	*157*	*170*	*92*

Tab. 4: Gesamtkosten des schwerwiegendsten Cyber-Angriffs der letzten 12 Monate nach Angriffsart und Beschäftigtengrößenklasse (avg = Mittelwert; med = Median; n = Anzahl der Beobachtungen; von Skarczinski et al. 2022b).

Mit Blick auf die entstandenen Schäden wiegen Kosten durch den Abfluss von finanziellen Mitteln (Durchschnitt: 31.500 EUR; Median: 5.000 EUR) und Kosten durch Betriebsunterbrechungen bzw. Umsatzverlusten (Durchschnitt: 23.400 EUR; Median: 3.000 EUR) am schwersten (vgl. Tab. 4). Auf Basis einer Gegenüberstellung bestehender und einschlägiger Literatur im Forschungsbeitrag D wird deutlich, dass im Vergleich zu kommerziellen Studien und Studien, die auf öffentlichen bzw. kommerziellen sog. „Operational-Risk-Datenbanken“ basieren, die analysierten Kosten tendenziell deutlich geringer ausfallen.

		External advise & support	Compensations & fines	Drain off financial means	Replacement & recovery	Defense & investigation / personnel costs	Business interruption / revenue loss
	avg	1.8k	2.3k	25.8k	12.6k	7.9k	10.6k
10-49	med	775	500	3.5k	1k	620	2k
	n	*92*	*5*	*6*	*111*	*124*	*66*
	avg	2k	952	47.6k	11.6k	15.4k	10.4k
50-99	med	1k	800	2k	900	1k	3k
	n	*103*	*3*	*9*	*108*	*121*	*55*
	avg	5.5k	10.6k	6.6k	21.6k	7.6k	23.3k
100-249	med	1k	6.5k	3.5k	1k	1k	5k
	n	*79*	*6*	*6*	*78*	*103*	*49*
	avg	4.5k	50k	16.5k	2.9k	13.8k	56.4k
250-499	med	1k	50k	13k	1k	1k	3k
	n	*74*	*1*	*3*	*76*	*104*	*53*
	avg	4k	27.7k	41.9k	8.8k	26.3k	14.5k
>500	med	2k	3k	25k	1k	2k	3.3k
	n	*29*	*3*	*8*	*47*	*63*	*22*
	avg	3.3k	11.7k	31.5k	11.8k	13k	23.4k
Total	med	1k	2.5k	5k	1k	1k	3k
	n	*377*	*18*	*32*	*420*	*515*	*245*

Tab. 5: Gesamtkosten des schwerwiegendsten Cyber-Angriffs der letzten 12 Monate nach Kostenart und Beschäftigtengrößenklasse (von Skarczinski et al. 2022b).

Forschungsbeitrag F (von Skarczinski et al. 2023) prüft verschiedene Verteilungsfunktionen, um die in Beitrag D deskriptiv dargestellten Kosten des schwerwiegendsten Angriffs der letzten 12 Monate stochastisch zu modellieren. Da die Kosten, wie in Beitrag D dargestellt, sehr ungleich bzw. extrem verteilt sind, da vielen Unternehmen gar keine oder geringe Kosten und nur sehr wenigen Unternehmen sehr hohe Kosten entstehen, ist es aus Cyber-Risiko-Management Perspektive besonders wichtig, das sog. „Tail-“ bzw. Rand-Verhalten der Verlustverteilungen zu analysieren und bestmöglich zu beschreiben. Da die Zielsetzung des Cyber-Risiko-Managements ist, durch die rechtzeitige Identifikation, Bewertung und Behandlung von Cyber-Risiken extreme und hohe Schäden von der Organisation abzuwenden, sind passende Verlustverteilungen für verschiedene unternehmens- und angriffsrelevante Merkmale (z.B. Beschäftigtengrößenklasse, Branchenzugehörigkeit, Angriffsart, etc.) essenziell.

Im Forschungsbeitrag wird zunächst eine modifizierte („tempered“) verallgemeinerte Extremwertverteilung (Generalized Extrem Value Distribution; GEV) (1) vorgestellt, die die Idee der temperierten verallgemeinerten Paretoverteilung (tempered Generalized Pareto Distribution, GDP) aufgreift und im Vergleich zur etablierten verallgemeinerten Extremwertverteilung von Beirlant (2004) neben dem formgebenden Parameter γ, dem Skalenparameter σ und dem Lageparameter μ, den zusätzlichen Parameter β nutzt, um die kumulative Verteilungsfunktion (Cumulative Distribution Function, CDF) mithilfe einer Exponentialfunktion zu temperieren.

$$G(x) = exp\left(-exp\left(-\frac{x-\mu}{\beta}\right)\left(1+\gamma\frac{x-\mu}{\sigma}\right)^{-1/\gamma}\right) \quad (1)$$

Anschließend werden, basierend auf den empirischen Kostendaten, die Parameter für vier verschiedene Kostenverteilungen (Lognormal, Weibull, GEV, modifizierte GEV) mithilfe der

Maximum-Likelihood-Methode geschätzt. Im visuellen Vergleich zeigt sich für die Gesamtstichprobe (N=805), dass die GEV und modifizierte GEV am rechten Rand („Tail“) der Verteilung deutlich näher an den empirischen Daten liegt, als die Lognormal- und Weibullverteilung (vgl. Abb. 10). Angewandte Chi-Quadrat Goodness-of-Fit-Tests (Snedecor und Cochran 1992) zeigen zudem, dass die GEV und die modifizierte GEV die empirischen Daten am besten modellieren, wobei die modifizierte GEV eine signifikante Teststatistik aufzeigt (α=5%).

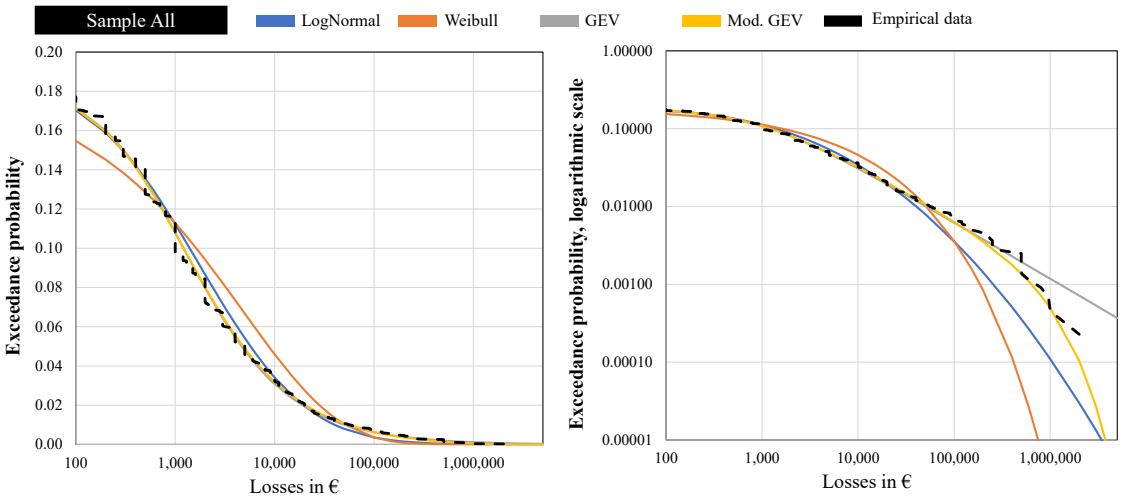

Abb. 10: Überlebensfunktionen der Gesamtstichprobe (N=805; Y-Achse ohne/mit logarithmischer Skala; von Skarczinski et al. 2023).

Für verschiedene Sub-Stichproben (Beschäftigtengrößenklasse (S=Size); Branchenzugehörigkeit (I=Industry); Kostenart (L=Loss type); Angriffsart (A=Attack type)) werden die geschätzten Parameter der Verteilungen dargestellt und mithilfe des Akaike Information Criterion (AIC) verglichen. Die Modellselektion mittels AIC bevorzugt die GEV und modifizierte GEV, welche insgesamt sehr nah zusammenliegen (vgl. Tab. 6). Auf Grundlage der modifizierten GEV-Verteilung, die neben der Verlustfunktion auch eine Überschreitungshäufigkeit impliziert, ist es möglich, die Verluste einzelner Unternehmen, aber auch die einer gesamten Wirtschaft abzuleiten.

Model	Parameter	All	S_1	S_5	I_Fin	I_Man	L_Rev	A_Ran	A_Phi
Losses ≤ 0	P	0.8163	0.8215	0.7794	0.8895	0.8088	0.9512	0.3304	0.5918
LogNormal	Mue	7.4617	7.1972	7.8831	6.7955	7.5181	7.9092	7.7443	7.3476
	Sigma	3.8467	3.6645	4.6409	3.4721	4.1791	3.4474	3.7339	3.8415
	AIC	*19569*	*4597*	*2299*	*509*	*5425*	***5973****	*4895*	*4001*
Weibull	Alpha	4872.24	3688.03	8051.65	2142.22	5459.29	7001.99	6279.59	4332.66
	Sigma	0.4532	0.4529	0.4494	0.6485	0.4296	0.5029	0.4815	0.4528
	AIC	*19835*	*4668*	*2320*	***508****	*5504*	*6026*	*4957*	*4060*
GEV	Mue	-719.16	-530.71	-722.29	-1134.96	-537.64	-1801.14	0.0000	-354.37
	Sigma	124.86	94.44	131.71	205.84	84.60	61.42	974.93	363.98
	Gamma	1.3820	1.3519	1.6820	0.7811	1.5804	1.2026	1.3526	1.3408
	AIC	*19535*	***4577****	*2298*	*509*	*5403*	*5974*	*4894*	***3989****
Modified GEV	Mue	-671.92	-487.62	-561.55	-49.89	-481.70	-1716.56	0.0000	-337.18
	Sigma	107.62	79.13	73.46	0.00	66.53	53.35	925.55	338.89
	Gamma	1.4587	1.4411	2.0322	6.2055	1.7080	1.2445	1.4635	1.4079
	Beta	926391	611030	298439	5269	766552	1910028	490909	882324
	AIC	***19531****	***4577****	***2296****	*509*	***5402****	*5975*	***4893****	*3990*

Tab. 6: Auswahl der Sub-Stichproben - Geschätzte Parameter und zugehöriges AIC (S_1: 10-49 Beschäftigte; S_2: >500 Beschäftigte; I_FIN: Industrie Finanzen; I_MAN: Industrie Herstellung; L_Rev: Umsatzverluste; A_Ran: Ransomware Angriff; A_Phi: Angriff; *geringster Wert je Spalte; von Skarczinski et al. 2023).

Auf Basis der modifizierten GEV der Gesamtstichprobe lässt sich dadurch ein durchschnittlicher Schaden von 3.648 EUR pro Jahr für jedes Unternehmen mit mehr als 9 Mitarbeitenden in Deutschland ermitteln. Für die 372.599 Unternehmen der deutschen Wirtschaft, die mehr als neun Beschäftigte haben, beträgt der erwartete durchschnittliche Schaden bzw. betragen die direkten Kosten durch Cyber-Angriffe pro Jahr 1,35 Milliarden Euro.

4 Diskussion von Implikationen und Limitationen

Nach der Zusammenfassung der wesentlichen Forschungsergebnisse mit Bezug zu den Einflussfaktoren sowie der Quantifizierung von Cyber-Risiken folgt eine Diskussion der Implikationen für Wissenschaft und Praxis inklusive zukünftiger Forschungsbedarfe. Zudem werden die Limitationen der Forschungsbeiträge kritisch gewürdigt.

4.1 Implikationen: Verfügbarkeit von Daten

Sowohl für die Erforschung von Einflussfaktoren als auch für die Quantifizierung von Cyber-Risiken, sind geeignete Daten von essentieller Bedeutung. In den vorangegangenen Kapiteln 1.2 und 2.4 und in den Forschungsbeiträgen C bis F wurde dargelegt, dass es **erstens** sowohl für die Wissenschaft als auch für die Praxis einen sehr großen Bedarf an zuverlässigen Daten zum Thema

Cyber-Risiko gibt und **zweitens** ein großer Teil der Erkenntnisse zum Thema Cyber-Risiko auf entweder kommerziellen Surveys, Intra-Organisations-Daten, Datensätzen mit geringen Stichprobengrößen oder öffentlichen/kommerziellen OpRisk-Datenbanken basiert, für die die Motivation der Datenerhebung, Repräsentativität, Vollständigkeit und Qualität der Daten nicht sichergestellt werden kann bzw. nicht immer transparent ist. Mit Blick auf Abbildung 2 fehlt es an verfügbaren Datensätzen, die die Aspekte „Threat", „Security", „Surface Exposure", „Compromise", „Asset Exposure" und „Harm" für die jeweiligen Perspektiven „Technology", „Organisation" und „People" vereinen. Die den Forschungsbeiträgen zugrundeliegenden Datensätze leisten aufgrund ihrer Repräsentativität, Qualität und Detailtiefe einen klaren und bedeutsamen Beitrag zum Stand der Forschung. Jedoch weisen auch diese Limitationen auf (siehe Kapitel 4.4) und können nicht das gesamte Spektrum der dargestellten Cyber-Risiko Aspekte abdecken.

Für die Praxis ergeben sich daraus zwei wesentliche Implikationen. **Zum einen** wird es für Unternehmen in Zeiten zunehmender digitaler Komplexität und der korrespondierenden „Informationsüberflutung" (Bandyopadhyay und Zafar 2017) darauf ankommen, die Kompetenz aufzubauen und aufrechtzuerhalten, relevante Informationen zu identifizieren, einzuordnen und für die eigenen Zwecke kritisch hinterfragen zu können (z.B. sind vorgebrachte Bedrohungs-/Vorfallsdaten vergleichbar oder Risikomodelle angemessen?). Diese Kompetenz ist erforderlich, um Cyber-Risiken innerhalb aller Prozesse und Systeme einer Organisation sowie entlang ihrer Wertschöpfungsketten effizient steuern zu können. **Zum anderen** bedarf es der Mithilfe der Unternehmen, die Cyber-Risiko-Informationslage durch das (anonymisierte) Bereitstellen von Echtdaten zu verbessern (z.B. Kooperationen mit Forschungseinrichtungen, Teilnahme an Arbeits- und Expertengruppen, wissenschaftlichen Befragungen und Panels, etc.).

Auch für die Wissenschaft ergeben sich Implikationen. **Zum einen** sollten Forschungsbeiträge noch klarer darstellen, was die hervorgebrachten Daten und Erkenntnisse leisten können und was nicht. Zum anderen ist es nötig, verstärkt die Interoperabilität von Forschungsergebnissen zu erhöhen, beispielsweise durch die (Weiter-)Entwicklung von Theorien, Konzepten und Messkonstrukten sowie deren Schnittstellen. Um eine umfassende Grundlage für die Messbarkeit der verschiedenen Aspekte von Cyber-Risiken zu erhalten, wird die verstärkte integrierte Anwendung multidisziplinärer Erhebungs- und Analysemethoden benötigt (z.B. explorative Analyse von SIEM/SOC Event-Logs, sozialpsychologische Analysen von Mitarbeitenden, Simulation finanzieller KPIs, etc.). **Zuletzt** sollten mehr wissenschaftliche Datensätze öffentlich zugänglich gemacht werden, was den Aufbau entsprechender Datenplattformen/Datenbanken, aber auch die Schaffung der vertraglichen und rechtlichen Grundlagen bereits bei der Datenerhebung beinhaltet.

4.2 Implikationen: Einflussfaktoren von Cyber-Risiken

Die Forschungsbeiträge A, B, C und E haben neue und empirisch begründete Erkenntnisse über die Einflussfaktoren von Cyber-Risiken hervorgebracht. Dass es weiterhin einen großen Forschungsbedarf gibt, zeigen die erarbeiteten Implikationen und nicht zuletzt auch die unbestätigten Hypothesen und kontra-intuitiven Ergebnisse innerhalb der Forschungsbeiträge. Beitrag A bestätigt basierend auf dem Routine-Activity-Approach, dass das Vorhandensein von Cyber-Kriminalität unter anderem vom routinemäßigen (Online-)Verhalten der Nutzer und

Nutzerinnen und der Abwesenheit fähiger Wächter (bzw. dem Vorhandensein von Schutzmaßnahmen) abhängt. Jedoch zeigten nicht alle theoriegeleiteten Faktoren einen empirischen Einfluss auf die Viktimisierung (z.B. das Alter der Nutzer und Nutzerinnen). Forschungsbeitrag B identifizierte Unternehmensmerkmale sowie technische und organisatorische Sicherheitsmaßnahmen, die einen Einfluss auf die Betroffenheit durch Cyber-Angriffe haben, jedoch lieferten längst nicht alle erwarteten Schutzmaßnahmen einen signifikanten Beitrag zur Betroffenheit. Auf Basis des TOE-Frameworks untersuchte Forschungsbeitrag C technologische, organisatorische und umweltbezogene Adaptionsfaktoren von Cyber-Versicherungen und identifizierte statistisch signifikante Adaptionsfaktoren in allen TOE-Dimensionen. Ein Großteil der theoriegeleiteten Einflussfaktoren blieb jedoch nur teilweise bestätigt oder unbestätigt und auch schwache bis moderate Bestimmtheitsmaße deuten darauf hin, dass es weitere Faktoren geben muss, die die Adaption von Cyber-Versicherungen erklären. Auch der Forschungsbeitrag E erbrachte neue und essentielle Erkenntnisse, in dem mittels eines PLS-Strukturgleichungsmodells die Beziehung verschiedener Einflussfaktoren auf die direkten Kosten von Cyber-Angriffen modelliert werden konnte. Jedoch gab es auch hier kontra-intuitive Ergebnisse, insofern, dass weder technische noch organisatorische Schutzmaßnahmen einen unmittelbaren Einfluss auf die direkten Kosten des schwerwiegendsten Angriffs hatten, sondern vor allem über die technischen Konsequenzen wirkten.

Wie bereits in einschlägiger Literatur postuliert (Eling 2020; Cresswell und Hassan 2007), ist Cyber-Risiko-Management ein hochgradig komplexes und dynamisches Forschungsfeld, in dem zahlreiche Faktoren auf technologischer, organisatorischer und behavioristischer Ebene zusammenwirken oder sich überlagern. Für die Wissenschaft ergeben sich daraus vier wesentliche Implikationen. **Erstens**, bedarf es konsistenter Cyber-Theorien, die das Phänomen umfassend beschreiben. Neben den in den Forschungsbeiträgen verwendeten Theorien wurden in der Literatur auch weitere Theorien zur Untersuchung von Cyber-Risiken und deren Einfluss auf die organisatorische Performance herangezogen (z.B. Organizational Learning: Kwon und Johnson 2014; Institutional Theory, Institutional Anomie Theory; Opportunity Theory of Crime: Sen und Borle 2015; Ressource-Based View: Weishäupl und Yasasin 2015), jedoch deckte bisher keine dieser Ansätze die technologischen, organisatorischen und behavioristischen Aspekte ganzheitlich ab. Damit einhergehend ist es, **zweitens**, erforderlich konsistente Standards und Konstrukte zur Messung von Cyber-Risiken zu etablieren. Das beinhaltet sowohl die Reife von Sicherheitsmaßnahmen mit Blick auf ihre präventive oder reaktive Wirkung gegenüber bestimmten Bedrohungen, als auch das Ausmaß von Schäden, welche nicht immer nur technischer oder finanzieller Natur sind. Ziel muss es an dieser Stelle sein, die Transparenz, wissenschaftliche Rigorosität und Vergleichbarkeit der Cyber-Risiko-Forschung zu erhöhen. **Drittens** wird es verstärkt von Nöten sein, dem komplexen Forschungsfeld Cyber-Risiko mit interdisziplinären Forschungsteams und Ansätzen zu begegnen. Neben der Informatik, der Wirtschaftsinformatik und den Wirtschaftswissenschaften sind vor allem die Disziplinen Kriminologie- und Sozialwissenschaften, Organisationswissenschaften, Rechtswissenschaften und das Aktuars- und Versicherungswesen relevante Bereiche. Da Cyber-Risiko noch ein relativ junges Forschungsfeld ist (Eling 2020), sollte als **vierte** Implikation für die Wissenschaft die Vermeidung des sog. Publication-Bias (Amrhein et al. 2019; Rothstein et al. 2005; Egger und Smith 1998) angestrebt werden, welches dafür sorgt, dass nicht oder nur schwach signifikante Forschungsergebnisse seltener veröffentlicht werden und so nicht zum „Body of Knowledge“ beitragen können.

Implikationen für die Praxis beinhalten, dass es Unterschiede in der Betroffenheit durch Cyber-Angriffe gibt und Unternehmen durchaus die Möglichkeit haben, sich zu schützen. Die nachhaltige

Sensibilisierung der Geschäftsführung und der Belegschaft für Informationssicherheit spielen eine entscheidende Rolle, die unermüdlich gefördert werden sollte, da die Vermeidung und Abwehr von Cyber-Angriffen schon lange keine ausschließliche Aufgabe der IT-Abteilungen ist. Da technische Sicherheitsmaßnahmen durch sog. Social-Engineering-Angriffe umgangen oder aufgrund mangelnder Usability nicht ausgeführt werden könnten, braucht es eine Änderung des Bewusstseins von Managern und Beschäftigten hinsichtlich der Informationssicherheit. Durch die zunehmende Digitalisierung in allen Lebensbereichen, kann dieser Bedarf eines stärkeren Informationssicherheits-Bewusstseins auch auf die gesamte Gesellschaft übertragen werden. Cyber-Risiko-Management als wichtiger Bestandteil der Informationssicherheit ist kein Trendthema, sondern notwendige Bedingung für die erfolgreiche Digitalisierung von Organisationen, Prozessen und Wertschöpfungsketten. Geschäftsführungen sollten aus Eigeninteresse an der sicheren Betriebsfortführung und nicht zuletzt wegen der Verschärfung regulatorischer Anforderungen und Haftungsrisiken hinterfragen, wie sie Cyber-Risiken identifizieren, bewerten und steuern.

4.3 Implikationen: Quantifizierung von Cyber-Risiken

Die Forschungsbeiträge D und F brachten wesentliche und empirisch begründete Erkenntnisse zu Häufigkeiten und direkten Kosten von Cyber-Angriffen hervor. Sie wiesen darauf hin, dass direkte Kosten zwischen verschiedenen Angriffsarten, Beschäftigtengrößenklassen und Unternehmensbranchen variieren, ungleich zwischen den Unternehmen verteilt sind und bestmöglich durch (modifizierte) Extremwertverteilungen modelliert werden können.
Für die Wissenschaft können daraus vier wesentliche Implikationen abgeleitet werden. **Erstens** bieten die in Forschungsbeitrag F vorgeschlagenen modifizierten Extremwertverteilungen eine probate stochastische Grundlage für eine Vielzahl von Anwendungsfällen, wie beispielweise die Berechnung betrieblicher Cyber-Risiko-Kennzahlen, die Bepreisung von Cyber-Versicherungen oder die Erstellung ökonomischer Modelle. Obwohl die vorgeschlagenen Verteilungsmodelle auf einer repräsentativen Zufallsstichprobe basieren, sollten sie durch weitere repräsentative Datensätze (z.B. aus anderen Regionen, durch andere Erhebungsinstrumente) validiert werden. **Zweitens** scheinen die analysierten Schäden durch Cyber-Angriffe im Vergleich zu den Ergebnissen kommerzieller Literatur oder Studien, die auf den Daten von öffentlichen/kommerziellen OpRisk-Datenbanken basieren, geringer auszufallen (vgl. Forschungsbeitrag D und F). Da eine direkte Vergleichbarkeit verwandter Literatur aufgrund der unterschiedlichen Systematisierung und Messung (z.B. unterschiedliche Grundgesamtheiten, Stichproben, Datenerhebungen, berücksichtige Kosten, Zeitpunkt, Zeitspanne, etc.) von Cyber-Schäden nicht ohne weiteres möglich ist, bedarf es Ansätzen und Studien auf Meta-Ebene, um den Umfang und den zeitlichen Verlauf des Phänomens erfassen zu können. Neben Studien zu Cyber-Schäden, die auf Befragungen oder technischen Vorfallsdaten beruhen, erscheint die Analyse von Daten des Rechnungswesens von Organisationen (z.B. CapEx, OpEx, Personalkosten, Outsourcing, Dienstleister, etc.) mit Blick auf Informationssicherheit aufschlussreich, um verstärkt die tatsächlichen betrieblichen Kosten in den Fokus zu nehmen. **Drittens** ergibt sich nach der Aufstellung der Cyber-Risiko-Modelle der Forschungsbedarf, wie diese optimal mit dem operativen Betrieb der Informationssicherheit und der IT in einer Organisation verknüpft werden können. Eine tatsächliche Steuerung der Informationssicherheit auf Basis von ermittelten Cyber-Risiken wird nur vorteilhaft sein, wenn sich eine Änderung der Einflussfaktoren „Threat“, „Surface Exposure“, „Security“, „Compromise“ und „Asset Exposure“ dynamisch und realitätsnah auf die betrachteten Cyber-Risiko-Kennzahlen auswirkt. Zum Beispiel sollte die

Investition in eine neue Firewall den Reifegrad der präventiven Sicherheit erhöhen und damit, bei sonst gleichen Bedingungen, das Risiko einer Malware-Infektion verringern. Damit könnte die Informationssicherheit nach dem Erreichen einer notwendigen Basissicherheit über das Kosten-Nutzen-Prinzip gesteuert werden. Schließlich sollte, **viertens**, verstärkt untersucht werden, wie Forschungsartefakte des Cyber-Risiko-Managements gestaltet und präsentiert werden sollten, um eine höhere Transferleistung von Forschungserkenntnissen in die Praxis sicherzustellen.
Auch für die Praxis ergeben sich Implikationen. **Erstens** können Unternehmen die Erkenntnisse aus den Forschungsbeitragen D und F als Benchmark oder Berechnungsgrundlage für das eigene Cyber-Risiko-Management nutzen. Beispielsweise könnten mithilfe der modifizierten Extremwertverteilungen Cyber-Risiko-Kennzahlen für den Lage- bzw. Geschäftsbericht im Rahmen des Jahres- bzw. Konzernabschlusses erstellt werden. **Zweitens** deuten die Forschungsergebnisse darauf hin, dass Cyber-Risiken extrem verteilt und deswegen auch schwierig zu steuern sind. So kann es sein, dass Unternehmen jahrelang keine wesentlichen Cyber-Vorfälle erleiden und unvermittelt durch ein seltenes Event mit sehr großem Schadensausmaß getroffen werden. Mediale Beispiele dafür sind die Metro AG, die nach einem Cyber-Angriff im Oktober 2022 von kalkulierten Schäden durch Umsatzausfälle, Ineffizienzen und Kostenerhöhungen im mittleren 2-stelligen Millionen-Euro-Bereich berichtete (Metro AG 2022), und die Continental AG, die nach einem Cyber-Angriff mit einem Datenabfluss von ca. 40 Terrabyte im Sommer 2022 eine Lösegeldforderung von 50 Mio USD erhielt (Holland 2022). Diese in den Medien präsenten Großereignisse sollten jedoch auch immer im Kontext der Größenstruktur der Unternehmen in Deutschland betrachtet werden, in welcher Unternehmen mit mehr als 250 Beschäftigten weniger als 0,5% aller Unternehmen ausmachen, und fast 90% aller Unternehmen weniger als 10 Mitarbeitende haben. Auch wenn die durchschnittlichen direkten Kosten des schwerwiegendsten Cyber-Angriffs der letzten 12 Monate mit Blick auf die ca. 370.000 Unternehmen in Deutschland mit mehr als 9 Mitarbeitenden, die die Grundgesamtheit der Datenbasis für Beitrag D und F bilden, mit 20.348 EUR zunächst relativ gering wirken, sollte die Praxis die Gefahren durch den Eintritt „extremer“ Cyber-Ereignisse nicht unterschätzen. **Drittens** und abschließend haben die Forschungsergebnisse gezeigt, dass das Phänomen Cyber-Risiko hoch komplex und dynamisch ist und ihm nicht sinnvoll mit einer linearen Fortschreibung historischer Risikomaße und korrespondierender Sicherheitsmaßnahmen begegnet werden kann. Im Zuge der immer stärkeren Digitalisierung und Vernetzung werden Unternehmen vermehrt darauf angewiesen sein, die relevanten Stellschrauben hinsichtlich Technologie, Organisation und Menschen zu identifizieren und mit Bezug zur Informationssicherheit zu steuern. Ein erster wichtiger Schritt dafür ist die innerbetriebliche Schaffung von Transparenz über die Reife bestehender Sicherheitsmaßnahmen, außerdem die Kenntnis der tatsächlichen Kosten des Betriebs der Informationssicherheit sowie die Bewertung von Schäden eigener Cyber-Vorfälle.

4.4 Limitationen

Wie jeder wissenschaftlichen Arbeit unterliegen auch die Forschungsergebnisse dieser Dissertation Limitationen. Auch wenn die einzelnen Forschungsbeiträge, inklusive ihrer Limitationen, bereits durch doppelt-blinde Begutachtungsprozesse unter Einbeziehung von Fachexperten und Fachexpertinnen hinsichtlich ihrer wissenschaftlichen Qualität geprüft wurden, werden im Folgenden die wichtigsten Limitationen zusammengefasst.
Fünf der sechs Forschungsbeiträge basieren auf Vorarbeiten und Datensätzen des vom Bundesministerium für Wirtschaft und Energie geförderten KFN-Forschungsprojektes „Cyberangriffe

gegen Unternehmen“. Der sechste Beitrag basiert auf Daten einer Kriminalitätsbefragung der Bevölkerung durch die Landeskriminalämter in Schleswig-Holstein und Niedersachsen. Da die wesentlichen Limitationen dieser quantitativen Forschung in der Erhebung und Güte der Daten liegen, treffen die Limitationen gemeinsam auf die Forschungsbeiträge zu.

Mit Blick auf die KFN-Forschungsdaten ist der CATI-Befragungsmethode inhärent, dass die Interviewpartner nur über die Cyber-Angriffe berichten konnten, die dem Unternehmen und dem Interviewpartner bekannt sind. Das sog. doppelte bzw. absolute Dunkelfeld kann generell mithilfe von Befragungen nicht erforscht werden. Aufgrund der Stichprobenzusammensetzung mit Fokus auf kleine und mittelständische Unternehmen (KMU) in Deutschland, sind die Forschungsergebnisse möglicherweise nicht auf andere Länder und Mikro-Unternehmen übertragbar. Zudem basieren die Analysen auf historischen Daten, die nicht zwangsläufig zukünftige Entwicklungen widerspiegeln. Durch die Befragung einer einzelnen Person, die stellvertretend für ein ganzes Unternehmen befragt wird, können die erhobenen Daten durch subjektive Einstellungen, Kenntnisse und Motivationen beeinflusst werden (sog. „Self-Reporting Bias“, „Social Desirability Bias“). Möglich ist auch, dass Interviewpartner aufgrund der sensiblen Informationen keine oder falsche Antworten gaben (sog. „(Non-)Response Bias“). Die angegebenen Kosten von Cyber-Angriffen wurden von den befragten Personen geschätzt. Außerdem könnte es andere wichtige Einflussfaktoren geben, die nicht erhoben wurden.

Für die Stichprobenziehung wurde auf zwei kommerzielle Unternehmensdatenbanken zugegriffen. Nach eigenen Angaben sollten die Unternehmensdatenbanken alle registrierten Unternehmen in Deutschland enthalten, die mehr als neun Mitarbeitende haben. Sollten diese Angaben nicht korrekt sein, ist es möglich, dass einige Unternehmen in der Grundgesamtheit nicht die Chance hatten, in die Zufallsstichprobe zu gelangen. Da die Struktur der Stichprobe in Bezug auf die Unternehmensbranchen und die Beschäftigtengrößenklassen der Grundgesamtheit entspricht, gibt es keine Hinweise auf strukturelle Verzerrungen. Jedoch kann die Möglichkeit einer Verzerrung durch Selbstselektion (sog. „Self-Selection Bias“) insofern, dass bestimmte Unternehmen nicht an Befragungen teilnehmen, nicht ausgeschlossen werden. Die genannten Limitationen des „Self-Reporting Bias“, „Social Desireability Bias“, „Self-Selection Bias“ und die Möglichkeit nicht im Datensatz enthaltener relevanter Variablen treffen auch auf den Datensatz der Landeskriminalämter in Schleswig-Holstein und Niedersachsen zu.

Neben den datenbezogenen Limitationen führt der Mangel an konsistenten Cyber-Risiko-Theorien und Konzepten dazu, dass es noch keine etablierten Messkonstrukte und Standards für die Analyse von Einflussfaktoren und Schäden von Cyber-Angriffen gibt (Eling 2020). Daher könnten die angewandten Operationalisierungen entsprechender Variablen in Zukunft hinterfragt, angepasst oder sogar verworfen werden.

5 Fazit

Auf Basis großer und repräsentativer Viktimisierungsbefragungen von Individuen und Unternehmen, untersucht diese Dissertation mithilfe quantitativer Forschungsmethoden die empirischen Einflussfaktoren von Cyber-Vorfällen bzw. Cyber-Angriffen und quantifiziert deren Auswirkungen. Die einzelnen Forschungsbeiträge identifizieren Schutz- und Risikofaktoren und zeigen auf, dass die direkten Kosten durch Cyber-Angriffe gegen Unternehmen extrem verteilt sind. Die Forschungserkenntnisse unterstützen Forschende und Unternehmen darin, Ansätze und Methoden zu entwickeln oder bestehende Strukturen zu validieren, um informierte, effiziente und wirtschaftliche Entscheidungen im Rahmen des betrieblichen Cyber-Risiko-Managements treffen zu können. Da ein Großteil bestehender Literatur zum Thema Cyber-Risiko und Schäden durch Cyber-Angriffe aus kommerziellen Studien besteht, kleine oder nicht repräsentative Stichproben aufweist oder sich auf eine deskriptive und undetaillierte Beschreibung der Auswirkungen beschränkt, tragen die Forschungsergebnisse dieser Dissertation nicht nur inhaltlich, sondern auch mit Blick auf die wissenschaftliche Rigorosität zum sog. „Body of Knowledge“ bei.

In Übereinstimmung mit der Literaturrecherche von Eling (2020), zeigen die Forschungsbeiträge auf, dass das Thema Cyber-Risiko ein hoch dynamisches und komplexes Phänomen mit mannigfaltigen Forschungslücken ist. Daher ist eine empirische Validierung der Forschungsergebnisse dieser Dissertation sowie die weitere quantitative und qualitative Forschung in den Bereichen Cyber-Risiko-Theorie und Operationalisierung, technologische, organisatorische und behavioristische Determinanten von Cyber-Risiken sowie dem stärkeren Verständnis von direkten und indirekten Schäden von Cyber-Angriffen nötig. Auch wenn das Thema Cyber-Risiko-Quantifizierung für viele Unternehmen in Deutschland, gerade mit Blick auf die kleinen- und mittelständischen Unternehmen, womöglich der Zeit voraus ist, sollten sich Geschäftsführungen und Entscheidungsträger fragen, ob sie Cyber-Risiken angemessen identifizieren und steuern. Ein erster wichtiger Schritt dazu ist die Schaffung von Transparenz über die eigene Reife der Informationssicherheit in Relation zur eigenen Geschäftstätigkeit.

Anhang A: Weitere Publikationen (nicht Teil der Dissertation)

Während des Zeitraumes der Promotion wurden weitere Veröffentlichungen mit Bezug zum Thema Cyber-Risiko veröffentlicht, an denen der Autor maßgebliche Anteile leistete.

#	Beitrag	Typ
1	Dreißigacker, Arne; **von Skarczinski, Bennet Simon**; Wollinger, Gina Rosa (2020b): Cyberangriffe gegen Unternehmen in Deutschland. Ergebnisse einer repräsentativen Unternehmensbefragung 2018/2019. Hannover (KFN-Forschungsbericht, 152). Online verfügbar unter https://kfn.de/wp-content/uploads/Forschungsberichte/FB_152.pdf, zuletzt geprüft am 28.05.2020. Kurzreferenz: (Dreißigacker et al. 2020b).	Forschungs-bericht
2	Dreißigacker, Arne; **von Skarczinski, Bennet Simon** (2020): Cyberangriffe gegen Unternehmen. Ergeb- nisse einer repräsentativen Unternehmensbefragung in Deutschland 2018/2019. Kurzbericht. Hg. v. Kriminologisches Forschungsinstitut Niedersachsen. Hannover. Online verfügbar unter https://kfn.de/wp-content/uploads/2020/03/Cyberangriffe%20gegen%20Unternehmen%20-%20Kurzbericht.pdf, zuletzt geprüft am 14.10.2023. Kurzreferenz: (Dreißigacker und von Skarczinski 2020).	Forschungs-bericht
3	Dreißigacker, Arne; **von Skarczinski, Bennet Simon**; Bergmann, Marie Christine; Wollinger, Gina Rosa (2020a): Cyberangriffe gegen private Internetnutzer*innen. In: Thomas-Gabriel Rüdiger und Petra Saskia Bayerl (Hg.): Cyberkriminologie. Wiesbaden: Springer Fachmedien Wiesbaden, S. 319–344. Kurzreferenz: (Dreißigacker et al. 2020a).	Fachbuch
4	Wollinger, Gina Rosa; Dreißigacker, Arne; **von Skarczinski, Bennet Simon** (2020): Formen der Bedrohung von Cyberkriminalität. In: Gina Rosa Wollinger und Anna Schulze (Hg.): Handbuch Cybersecurity für die öffentliche Verwaltung. Wiesbaden: Kommunal- und Schul-Verlag (KSV Verwaltungspraxis), S. 27–56. Kurzreferenz: (Wollinger et al. 2020).	Fachbuch
5	Dreißigacker, Arne; **von Skarczinski, Bennet Simon**; Wollinger, Gina Rosa (2020d): Im Visier: Repräsentative Studie zur Cyberkriminalität in deutschen Unternehmen. In: iX – Magazin für professionelle Informationstechnik (6), S. 78–81. Online verfügbar unter https://www.heise.de/select/ix/2020/6/1910510321680924430, zuletzt geprüft am 14.10.2023. Kurzreferenz: (Dreißigacker et al. 2020d).	Fach-zeitschrift
6	Dreißigacker, Arne; **von Skarczinski, Bennet Simon**; Wollinger, Gina Rosa (2020c): Cyberangriffe gegen Unternehmen: Erste Ergebnisse einer repräsentativen Unternehmensbefragung in Deutschland. In: Christian Grafl, Monika Stempkowski, Katharina Beclin und Isabel Haider (Hg.): "Sag, wie hast du's mit der Kriminologie?". Die Kriminologie im Gespräch mit ihren Nachbardisziplinen. Mönchengladbach: Forum Verlag Godesberg (Neue Kriminologische Schriftenreihe, 118), S. 933–952. Kurzreferenz: (Dreißigacker et al. 2020c).	Fachbuch

7	Huaman, Nicolas; Krause, Alexander; **von Skarczinski, Bennet Simon**; Stransky, Christian; Wermke, Dominik; Acar, Yasemin et al. (2021a): Cybercrime in Small and Medium-sized Enterprises. SOUPS 2021 Posters. Forschungsposter. Hg. v. SOUPS. Online verfügbar unter https://www.usenix.org/system/files/soups21-poster62-huaman-cybercrime.pdf, zuletzt geprüft am 14.10.2023. (Huaman et al. 2021a).	Forschungs-poster
8	Dreißigacker, Arne; **von Skarczinski, Bennet Simon**; Wollinger, Gina Rosa (2021b): Cyberangriffe gegen Unternehmen in Deutschland. Ergebnisse einer Folgebefragung 2020. Hannover: Kriminologisches Forschungsinstitut Niedersachsen e.V. (KFN) (Forschungsbericht / KFN, Kriminologisches Forschungsinstitut Niedersachsen e.V, Nr. 162). Kurzreferenz: (Dreißigacker et al. 2021b).	Forschungs-bericht
9	Dreißigacker, Arne; Fahl, Sascha; Huaman, Nicolas; **von Skarczinski, Bennet Simon**; Stransky, Christian; Wollinger, Gina Rosa (2021a): Cyberangriffe gegen Unternehmen - Projektabschlussbericht. MBWi-VID5-090168623-01-1/2017. Hannover: Kriminologisches Forschungsinstitut Niedersachsen e.V. (KFN); Leibniz Universität Hannover - Forschungszentrum L3S. Online verfügbar unter https://kfn.de/wp-content/uploads/2022/01/BMWi-VID5-090168623-01-1-2017%20Projektabschlussbericht.pdf. Kurzreferenz: (Dreißigacker et al. 2021a).	Forschungs-bericht
10	PricewaterhouseCoopers GmbH WPG (PwC) (2022): PwC's Global Automotive Cyber Security Management System (CSMS) Survey 2022. Pedal to the Metal − How to Navigate the Way to Automotive Cybersecurity. Online verfügbar unter https://www.pwc.de/en/cyber-security/global-automotive-cyber-security-management-system-survey.html, zuletzt geprüft am 14.10.2023. Kurzreferenz: (PwC 2022).	Survey-Report
11	Dreißigacker, Arne; **von Skarczinski, Bennet Simon**; Wollinger, Gina Rosa (2023): Unternehmen als Opfer von Cyberkriminalität. In: Thomas-Gabriel Rüdiger und P. Saskia Bayerl (Hg.): Handbuch Cyberkriminologie 2. Wiesbaden: Springer Fachmedien Wiesbaden (Cyberkriminologie – Theorien, Methoden, Erscheinungsformen), S. 587–609. Kurzreferenz: (Dreißigacker et al. 2023).	Fachbuch

Literaturverzeichnis

Akaike, Hirotugu (1974): A new look at the statistical model identification. In: *IEEE Trans. Automat. Contr.* 19 (6), S. 716–723. DOI: 10.1109/TAC.1974.1100705.

Aldasoro, Iñaki; Gambacorta, Leonardo; Giudici, Paolo; Leach, Thomas (2020): The drivers of cyber risk. BIS Working Papers No 865. Hg. v. Bank for International Settlements (BIS) (BIS Working Papers, 865). Online verfügbar unter https://www.bis.org/publ/work865.pdf.

Allianz Global Corporate & Specialty SE (Allianz) (2022): Allianz Risk Barometer 2022. The most important business risks for the next 12 months and beyond, based on the insight of 2,650 risk management experts from 89 countries and territories. Allianz. Online verfügbar unter https ://www.agcs.allianz.com/content/dam/onemarketing/agcs/ agcs/reports/Allianz-Risk-Barometer-2020.pdf, zuletzt geprüft am 05.04.2022.

Allianz Global Corporate & Specialty SE (Allianz) (2023): Allianz Risk Barometer. Identifying the major business risks for 2023. Online verfügbar unter https://www.allianz.com/content/dam/onemarketing/azcom/Allianz_com/press/document/Allianz-Risk-Barometer-2023.pdf, zuletzt geprüft am 01.08.2023.

Amrhein, Valentin; Greenland, Sander; McShane, Blake (2019): Scientists rise up against statistical significance. In: *Nature* 567 (7748), S. 305–307. DOI: 10.1038/d41586-019-00857-9.

Anderson, Ross; Barton, Chris; Böhme, Rainer; Clayton, Richard; Ganan, Carlos; Grasso, Tom et al. (2019): Measuring the Changing Cost of Cybercrime. In: *The 18th Annual Workshop on the Economics of Information Security*. DOI: 10.17863/CAM.41598.

Bandyopadhyay, Tridib; Mookerjee, Vijay S.; Rao, Ram C. (2009): Why IT managers don't go for cyber-insurance products. In: *Commun ACM* 52 (11), S. 68–73. DOI: 10.1145/1592761.1592780.

Bandyopadhyay, Tridib; Zafar, Humayun (2017): Influence of Information Overload on IT Security Behavior: A Theoretical Framework. In: *Americas Conference on Information Systems* 23. Online verfügbar unter https://core.ac.uk/download/pdf/301371895.pdf, zuletzt geprüft am 14.10.2023.

Beirlant, Jan; Goegebeur, Yuri; Segers, Johan; Teugels, Jozef L. (2004): Statistics of extremes. Theory and applications. Chichester: Wiley (Wiley series in probability and statistics). Online verfügbar unter http://www.loc.gov/catdir/description/wiley042/2004051046.html.

Benitez, Jose; Henseler, Jörg; Castillo, Ana; Schuberth, Florian (2020): How to perform and report an impactful analysis using partial least squares: Guidelines for confirmatory and explanatory IS research. In: *Inf Manag* 57 (2). DOI: 10.1016/j.im.2019.05.003.

Bergmann, Marie Christine; Dreißigacker, Arne; von Skarczinski, Bennet Simon; Wollinger, Gina Rosa (2018): Cyber-Dependent Crime Victimization: The Same Risk for Everyone? In: *Cyberpsychology, behavior and social networking* 21 (2), S. 84–90. DOI: 10.1089/cyber.2016.0727.

Beirlant, Jan; Goegebeur, Yuri; Segers, Johan; Teugels, Jozef L. (2004): Statistics of extremes. Theory and applications. Chichester: Wiley (Wiley series in probability and statistics). Online verfügbar unter http://www.loc.gov/catdir/description/wiley042/2004051046.html.

Biener, Christian; Eling, Martin; Wirfs, Jan Hendrik (2015): Insurability of Cyber Risk: An Empirical Analysis. In: *The Geneva Papers on Risk and Insurance - Issues and Practice* 40 (1), S. 131–158. DOI: 10.1057/gpp.2014.19.

Böhme, Rainer; Schwartz, Galina; others (2010): Modeling Cyber-Insurance: Towards a Unifying Framework. In: Workshop on the Economics of Information Security (WEIS). Harvard, June 2010.

Branley-Bell, Dawn; Coventry, Lynne; Briggs, Pam (2022): Cyber Insurance from the stakeholder's perspective. In: Proceedings of the 2022 European Symposium on Usable Security. EuroUSEC 2022: 2022 European Symposium on Usable Security. Karlsruhe Germany, 29 09 2022 30 09 2022. New York, NY, USA: ACM, S. 151–159.

Buil-Gil, David; Lord, Nicholas; Barrett, Emma (2021): The Dynamics of Business, Cybersecurity and Cyber-Victimization. Foregrounding the Internal Guardian in Prevention. In: *Vict Offender* 16 (3), S. 286–315. DOI: 10.1080/15564886.2020.1814468.

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2021): ISMS.1: Sicherheitsmanagement. Online verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/01_ISMS_Sicherheitsmanagement/ISMS_1_Sicherheitsmanagement_Edition_2021.pdf?__blob=publicationFile&v=2, zuletzt aktualisiert am 01.02.2021, zuletzt geprüft am 14.10.2023.

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2022): BSI warnt vor dem Einsatz von Kaspersky-Virenschutzprodukten. Online verfügbar unter https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/Presse-Archiv/220315_Kaspersky-Warnung.html?nn=1029964, zuletzt geprüft am 12.08.2023.

Bundeskriminalamt (BKA) (2022): Cybercrime - Bundeslagebild 2021. Online verfügbar unter https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2021.html?nn=28110, zuletzt geprüft am 12.08.2023.

Cohen, Fred; Phillips, Cynthia; Painton Swiler, Laura; Gaylor, Timothy; Leary, Patricia; Rupley, Fran; Isler, Richard (1998): A cause and effect model of attacks on information systems. In: *Comput Secur* 17 (3), S. 211–221. DOI: 10.1016/S0167-4048(98)80312-X.

Cohen, Lawrence E.; Felson, Marcus (1979): Social Change and Crime Rate Trends: A Routine Activity Approach. In: *Am Sociol Rev* 44 (4), S. 588. DOI: 10.2307/2094589.

Coles, Stuart (2001): An Introduction to Statistical Modeling of Extreme Values. London: Springer (Springer eBook Collection Mathematics and Statistics). Online verfügbar unter http://swbplus.bsz-bw.de/bsz40467836xcov.htm.

Cremer, Frank; Sheehan, Barry; Fortmann, Michael; Kia, Arash N.; Mullins, Martin; Murphy, Finbarr; Materne, Stefan (2022): Cyber risk and cybersecurity: a systematic review of data availability. In: *Geneva Pap Risk Insur Issues Pract* 47 (3), S. 698–736. DOI: 10.1057/s41288-022-00266-6.

Cresswell, Anthony; Hassan, Shahidul (2007): Organizational Impacts of Cyber Security Provisions: A Sociotechnical Framework. In:. 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07). Waikoloa, HI, USA, 03.01.2007 - 06.01.2007: IEEE, S. 98.

Dambra, Savino; Bilge, Leyla; Balzarotti, Davide (2020): SoK: Cyber Insurance – TechnicalChallenges and a System Security Roadmap. In: *IEEE Symposium on Security & Privacy*.

DePietro, Rocco; Wiarda, Edith; Fleischer, Mitchell (1990): The context for change: Organization, technology and environment. In: Louis G. Tornatzky und Mitchell Fleischer (Hg.): The processes of technological innovation. Lexington, MA: Lexington Books, S. 151–175.

Dreißigacker, Arne; Fahl, Sascha; Huaman, Nicolas; von Skarczinski, Bennet Simon; Stransky,

Christian; Wollinger, Gina Rosa (2021a): Cyberangriffe gegen Unternehmen - Projektabschlussbericht. MBWi-VID5-090168623-01-1/2017. Hannover: Kriminologisches Forschungsinstitut Niedersachsen e.V. (KFN); Leibniz Universität Hannover - Forschungszentrum L3S. Online verfügbar unter https://kfn.de/wp-content/uploads/2022/01/BMWi-VID5-090168623-01-1-2017%20Projektabschlussbericht.pdf.

Dreißigacker, Arne; von Skarczinski, Bennet Simon (2020): Cyberangriffe gegen Unternehmen. Ergeb- nisse einer repräsentativen Unternehmensbefragung in Deutschland 2018/2019. Kurzbericht. Hg. v. Kriminologisches Forschungsinstitut Niedersachsen. Hannover. Online verfügbar unter https://kfn.de/wp-content/uploads/2020/03/Cyberangriffe%20gegen%20Unternehmen%20-%20Kurzbericht.pdf, zuletzt geprüft am 14.10.2023.

Dreißigacker, Arne; von Skarczinski, Bennet Simon; Bergmann, Marie Christine; Wollinger, Gina Rosa (2020a): Cyberangriffe gegen private Internetnutzer*innen. In: Thomas-Gabriel Rüdiger und Petra Saskia Bayerl (Hg.): Cyberkriminologie. Wiesbaden: Springer Fachmedien Wiesbaden, S. 319–344.

Dreißigacker, Arne; von Skarczinski, Bennet Simon; Wollinger, Gina Rosa (2020b): Cyberangriffe gegen Unternehmen in Deutschland. Ergebnisse einer repräsentativen Unternehmensbefragung 2018/2019. Hannover (KFN-Forschungsbericht, 152). Online verfügbar unter https://kfn.de/wp-content/uploads/Forschungsberichte/FB_152.pdf, zuletzt geprüft am 28.05.2020.

Dreißigacker, Arne; von Skarczinski, Bennet Simon; Wollinger, Gina Rosa (2020c): Cyberangriffe gegen Unternehmen: Erste Ergebnisse einer repräsentativen Unternehmensbefragung in Deutschland. In: Christian Grafl, Monika Stempkowski, Katharina Beclin und Isabel Haider (Hg.): "Sag, wie hast du's mit der Kriminologie?". Die Kriminologie im Gespräch mit ihren Nachbardisziplinen. Mönchengladbach: Forum Verlag Godesberg (Neue Kriminologische Schriftenreihe, 118), S. 933–952.

Dreißigacker, Arne; von Skarczinski, Bennet Simon; Wollinger, Gina Rosa (2020d): Im Visier: Repräsentative Studie zur Cyberkriminalität in deutschen Unternehmen. In: *iX – Magazin für professionelle Informationstechnik* (6), S. 78–81. Online verfügbar unter https://www.heise.de/select/ix/2020/6/1910510321680924430, zuletzt geprüft am 14.10.2023.

Dreißigacker, Arne; von Skarczinski, Bennet Simon; Wollinger, Gina Rosa (2021b): Cyberangriffe gegen Unternehmen in Deutschland. Ergebnisse einer Folgebefragung 2020. Hannover: Kriminologisches Forschungsinstitut Niedersachsen e.V. (KFN) (Forschungsbericht / KFN, Kriminologisches Forschungsinstitut Niedersachsen e.V, Nr. 162).

Dreißigacker, Arne; von Skarczinski, Bennet Simon; Wollinger, Gina Rosa (2023): Unternehmen als Opfer von Cyberkriminalität. In: Thomas-Gabriel Rüdiger und P. Saskia Bayerl (Hg.): Handbuch Cyberkriminologie 2. Wiesbaden: Springer Fachmedien Wiesbaden (Cyberkriminologie – Theorien, Methoden, Erscheinungsformen), S. 587–609.

Edwards, Benjamin; Hofmeyr, Steven; Forrest, Stephanie (2016): Hype and heavy tails: A closer look at data breaches. In: *J Cybersecur* 2 (1), S. 3–14. DOI: 10.1093/cybsec/tyw003.

Egger, M.; Smith, G. D. (1998): Bias in location and selection of studies. In: *BMJ* 316 (7124), S. 61–66. DOI: 10.1136/bmj.316.7124.61.

EIOPA (2018): Understanding Cyber Insurance - A Structured Dialogue with Insurance Companies. Luxembourg. Online verfügbar unter https://www.eiopa.europa.eu/sites/default/files/publications/reports/eiopa_understanding_cyber_insurance.pdf, zuletzt geprüft am 15.11.2020.

Eling, Martin (2020): Cyber risk research in business and actuarial science. In: *Eur. Actuar. J.* 10

(2), S. 303–333. DOI: 10.1007/s13385-020-00250-1.

Eling, Martin; Wirfs, Jan (2019): What are the actual costs of cyber risk events? In: *Eur J Oper Res* 272 (3), S. 1109–1119. DOI: 10.1016/j.ejor.2018.07.021.

Emerald Publishing (2023): Organizational Cybersecurity Journal: Practice, Process and People. Online verfügbar unter https://www.emeraldgrouppublishing.com/journal/ocj, zuletzt geprüft am 07.09.2023.

EU (14.12.2022): Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie). NIS-2-Richtlinie. Fundstelle: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32022L2555. In: *Amtsblatt der Europäischen Union* (L333/80). Online verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32022L2555, zuletzt geprüft am 12.08.2023.

European Commission (EU-Commission) (2023): Cyber Resilience Act. Online verfügbar unter https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act, zuletzt aktualisiert am 20.06.2023, zuletzt geprüft am 12.08.2023.

European Union Agency for Cybersecurity (ENISA) (2017): ENISA overview of cybersecurity and related terminology. ENISA. Online verfügbar unter https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology, zuletzt aktualisiert am 2017, zuletzt geprüft am 21.12.2020.

European Union Agency for Cybersecurity (ENISA) (2023): ENISA Glossary. Online verfügbar unter https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/glossary, zuletzt geprüft am 01.08.2023.

Fahey, Liam; Narayanan, V. K. (1986): Macroenvironmental analysis for strategic management. St. Paul, MN: West Publishing Company (The west series in strategic management).

Fettke, Peter (2006): State-of-the-Art des State-of-the-Art. In: *Wirtsch. Inform.* 48 (4). DOI: 10.1007/s11576-006-0057-3.

Guembe, Blessing; Azeta, Ambrose; Misra, Sanjay; Osamor, Victor; Fernandez-Sanz, Luis; Pospelova, Vera (2022). The Emerging Threat of Ai-driven Cyber Attacks: A Review. Applied Artificial Intelligence, 36(1). https://doi.org/10.1080/08839514.2022.2037254.

Heinzl, Armin; Schoder, Detlef; Ulrich, Frank (2008): WI-Orientierungslisten. WI-Journalliste 2008 sowie WI-Liste der Konferenzen, Proceedings und Lecture Notes 2008. In: *Wirtschaftsinformatik* 50 (2), 155–163.

Herath, Tejaswini C.; Herath, Hemantha S. B.; D'Arcy, John (2020): Organizational Adoption of Information Security Solutions. In: *ACM SIGMIS Database for Advances in Information Systems* 51 (2), S. 12–35. DOI: 10.1145/3400043.3400046.

Hevner, Alan R.; March, Salvatore T.; Park, Jinsoo; Ram, Sudha (2004): Design Science in Information Systems Research. In: *MIS Q* 28 (1), S. 75–105.

Holland, Martin (2022): Continental: IT-Einbruch erfolgte über heruntergeladenen Browser von Mitarbeiter. Hg. v. Heise Online. Online verfügbar unter https://www.heise.de/news/Continental-IT-Einbruch-erfolgte-ueber-heruntergeladenen-Browser-von-Mitarbeiter-7394151.html, zuletzt aktualisiert am 14.12.2022, zuletzt geprüft am 14.10.2023.

Huaman, Nicolas; Krause, Alexander; von Skarczinski, Bennet Simon; Stransky, Christian; Wermke, Dominik; Acar, Yasemin et al. (2021a): Cybercrime in Small and Medium-sized

Enterprises. SOUPS 2021 Posters. Forschungsposter. Hg. v. SOUPS. Online verfügbar unter https://www.usenix.org/system/files/soups21-poster62-huaman-cybercrime.pdf, zuletzt geprüft am 14.10.2023.

Huaman, Nicolas; von Skarczinski, Bennet Simon; Wermke, Dominik; Stransky, Christian; Acar, Yasemin; Dreißigacker, Arne; Fahl, Sascha (2021b): A Large-Scale Interview Study on Information Security in and Attacks against Small and Medium-sized Enterprises. In: *Proceedings of the 30th USENIX Security Symposium*.

ISO/IEC 27005:2022(en), 2022-10: Information security, cybersecurity and privacy protection — Guidance on managing information security risks.

Jung, Kwangmin (2021): Extreme Data Breach Losses: An Alternative Approach to Estimating Probable Maximum Loss for Data Breach Risk. In: *North American Actuarial Journal* 25 (4), S. 580–603. DOI: 10.1080/10920277.2021.1919145.

Kshetri, Nir (2020): The evolution of cyber-insurance industry and market: An institutional analysis. In: *Telecommunications Policy* 44 (8), S. 102007. DOI: 10.1016/j.telpol.2020.102007.

Kuypers, Marshall; Paté-Cornell, Elisabeth; Maillart, Thomas (2016): An Empirical Analysis of Cyber Security Incidents at a Large Organization. Hg. v. Stanford University. Freeman Spogli Institute for International Studies. Online verfügbar unter https://fsi.stanford.edu/publication/empirical-analysis-cyber-security-incidents-large-organization.

Kwon, Juhee; Johnson, M. Eric (2014): Proactive Versus Reactive Security Investments in the Healthcare Sector. In: *MIS Q* 38 (2), S. 451–471.

Legner, Christine; Eymann, Torsten; Hess, Thomas; Matt, Christian; Böhmann, Tilo; Drews, Paul et al. (2017): Digitalization: Opportunity and Challenge for the Business and Information Systems Engineering Community. In: *Bus Inf Syst Eng* 59 (4), S. 301–308. DOI: 10.1007/s12599-017-0484-2.

Marotta, Angelica; Martinelli, Fabio; Nanni, Stefano; Orlando, Albina; Yautsiukhin, Artsiom (2017): Cyber-insurance survey. In: *Computer Science Review* 24, S. 35–61. DOI: 10.1016/j.cosrev.2017.01.001.

Matthiesen, Nils (2022): BSI-Warnung trifft Kaspersky offenbar hart. Hg. v. Imtest. Online verfügbar unter https://www.imtest.de/278285/news/bsi-warnung-trifft-kaspersky-offenbar-hart, zuletzt aktualisiert am 15.09.2022, zuletzt geprüft am 12.08.2023.

Mayring, Philipp (2014): Qualitative content analysis: theoretical foundation, basic procedures and software solution. Klagenfurt: Social Science Open Access Repository (SSOAR). Online verfügbar unter https://nbn-resolving.org/urn:nbn:de:0168-ssoar-395173.

Metro AG (2022): Nachtragsbericht - Ereignisse nach dem Bilanzstichtag. Cyberangriff. Online verfügbar unter https://berichte.metroag.de/geschaeftsbericht/2021-2022/zusammengefasster-lagebericht/nachtrags-und-prognosebericht/nachtragsbericht.html, zuletzt aktualisiert am 14.12.2022, zuletzt geprüft am 14.10.2023.

Myers, Michael D. (1997): Qualitative Research in Information Systems. Archival Version: Association for Information Systems (AISWorld) Section on Qualitative Research in Information Systems, updated version, last modified: September 4, 2018. Association for Information Systems (AISWorld) Section on Qualitative Research in Information Systems, updated version, last modified: September 4, 2018 www.qual.auckland.ac.nz. In: *MIS Q* 21 (2), S. 241–242. Online verfügbar unter http://www.misq.org/supplements/.

National Institute of Standards and Technology (NIST) (2023): NIST Glossary. Online verfügbar unter https://csrc.nist.gov/glossary/term/cyber_risk, zuletzt geprüft am 01.08.2023.

Openkritis (2023): EU NIS 2 Cybersecurity. Hg. v. Paul Weissmann. Online verfügbar unter https://www.openkritis.de/it-sicherheitsgesetz/eu-nis-2-direktive-kritis.html, zuletzt geprüft am 12.08.2023.

Orlikowski, Wanda J.; Baroudi, Jack J. (1991): Studying Information Technology in Organizations: Research Approaches and Assumptions. In: *Inf Sys Res* 2 (1), S. 1–28. DOI: 10.1287/isre.2.1.1.

Paoli, Letizia; Visschers, Jonas; Verstraete, Cedric (2018): The impact of cybercrime on businesses: a novel conceptual framework and its application to Belgium. In: *Crime Law Soc Chang* 70 (4), S. 397–420. DOI: 10.1007/s10611-018-9774-y.

Pate-Cornell, M.-Elisabeth; Kuypers, Marshall A. (2021): A Probabilistic Analysis of Cyber Risks. In: *IEEE Trans. Eng. Manage.* 70 (1), S. 3–13. DOI: 10.1109/TEM.2020.3028526.

PricewaterhouseCoopers GmbH WPG (PwC) (2022): PwC's Global Automotive Cyber Security Management System (CSMS) Survey 2022. Pedal to the Metal − How to Navigate the Way to Automotive Cybersecurity. Online verfügbar unter https://www.pwc.de/en/cyber-security/global-automotive-cyber-security-management-system-survey.html, zuletzt geprüft am 14.10.2023.

Rantala, Ramona (2008): Cybercrime against Businesses, 2005. Hg. v. U.S. Department of Justice. U.S. Department of Justice. Washington DC, USA (Bureau of Justice Statistics, Special Report).

Richards, Kelly (2009): Australian business assessment of computer user security. A national survey. Canberra, A.C.T.: Australian Institute of Criminology (AIC reports. Research and public policy series, 102).

Romanosky, Sasha (2016): Examining the costs and causes of cyber incidents. In: *J Cybersecur* 2 (2), 121-135. DOI: 10.1093/cybsec/tyw001.

Romanosky, Sasha; Ablon, Lillian; Kuehn, Andreas; Jones, Therese (2019): Content analysis of cyber insurance policies: how do carriers price cyber risk? Journal of Cybersecurity, 5(1). In: *J Cybersecur* 5 (1). DOI: 10.1093/CYBSEC/TYZ002.

Rothstein, Hannah R.; Sutton, Alexander J.; Borenstein, Michael (2005): Publication Bias in Meta-Analysis. Chichester, UK: John Wiley & Sons, Ltd.

Rüegg-Stürm, Johannes (2013): Das neue St. Galler Management-Modell. Grundkategorien einer integrierten Managementlehre; der HSG-Ansatz. 2., durchges.u. korr. Aufl, [Nachdr.]. Bern, Stuttgart, Wien: Haupt.

Sen, Ravi; Borle, Sharad (2015): Estimating the Contextual Risk of Data Breach. An Empirical Approach. In: *J Manag Inf Syst* 32 (2), S. 314–341. DOI: 10.1080/07421222.2015.1063315.

Snedecor, George W.; Cochran, William G. (1992): Statistical methods. 8. ed., 3. print. Ames, Iowa: Iowa State Univ. Press.

Straub, Detmar; Gefen, David (2004): Validation Guidelines for IS Positivist Research. In: *Commun Assoc Inf Syst* 13. DOI: 10.17705/1CAIS.01324.

Strupczewski, Grzegorz (2019): What Is the Worst Scenario? Modeling Extreme Cyber Losses. In: Philip Linsley, Philip Shrives und Monika Wieczorek-Kosmala (Hg.): Multiple Perspectives in Risk and Risk Management. Cham: Springer International Publishing (Springer Proceedings in Business and Economics), S. 211–230.

Thommen, Jean-Paul; Achleitner, Ann-Kristin (Hg.) (2012): Allgemeine Betriebswirtschaftslehre. Umfassende Einführung aus managementorientierter Sicht. 7., vollst. überarb. Aufl. Wiesbaden: Springer Gabler (Lehrbuch).

UK Department for Culture, Media and Sport (DCMS) (2022): Cyber Security Breaches Survey 2022. DCMS. Online verfügbar unter https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022, zuletzt aktualisiert am 11.07.2022, zuletzt geprüft am 30.12.2022.

Verband der Hochschullehrerinnen und Hochschullehrer für Betriebswirtschaft e.V. (VHB) (2022): Liste der Fachzeitschriften in VHB-JOURQUAL3. Online verfügbar unter https://vhbonline.org/vhb4you/vhb-jourqual/vhb-jourqual-3/gesamtliste, zuletzt geprüft am 05.09.2023.

Verband der Hochschullehrerinnen und Hochschullehrer für Betriebswirtschaft e.V. (VHB) (2024): VHB Publication Media Rating 2024. Online verfügbar unter https://vhbonline.org/en/service/vhb-rating-2024/

von Skarczinski, Bennet Simon; Boll, Lukas; Teuteberg, Frank (2021): Understanding the adoption of cyber insurance for residual risks - An empirical large-scale survey on organizational factors of the demand side. In: *ECIS Proceedings* (72). Online verfügbar unter https://aisel.aisnet.org/ecis2021_rp/72.

von Skarczinski, Bennet Simon; Dreissigacker, Arne; Teuteberg, Frank (2022a): More Security, less Harm? Exploring the Link between Security Measures and Direct Costs of Cyber Incidents within Firms using PLS-PM. In: *Wirtschaftsinformatik 2022 Proceedings* (2). Online verfügbar unter https://aisel.aisnet.org/wi2022/it_strategy/it_strategy/2.

von Skarczinski, Bennet Simon; Dreißigacker, Arne; Teuteberg, Frank (2022b): Toward enhancing the information base on costs of cyber incidents: implications from literature and a large-scale survey conducted in Germany. In: *OCJ*. DOI: 10.1108/OCJ-08-2021-0020.

von Skarczinski, Bennet Simon; Raschke, Mathias; Teuteberg, Frank (2023): Modelling maximum cyber incident losses of German organisations: an empirical study and modified extreme value distribution approach. In: *Geneva Pap Risk Insur Issues Pract* 48 (2), S. 463–501. DOI: 10.1057/s41288-023-00293-x.

Webster, Jane; Watson, Richard T. (2002): Analyzing the past to prepare for the future: Writing a literature review. In: *MIS Q* 26 (2), S. xiii–xxiii.

Weishäupl, Eva; Yasasin, Emrah (2015): IT Security Investments through the Lens of the Resource-based View: A new theoretical Model and Literature Review. In: Twenty-Third European Conference on Information Systems. Münster, Germany.

Weishäupl, Eva; Yasasin, Emrah; Schryen, Guido (2018) 'Information security investments: An exploratory multiple case study on decision-making, evaluation and learning', Computers & Security, 77, pp. 807–823. doi: 10.1016/j.cose.2018.02.001.

Wheatley, Spencer; Hofmann, Annette; Sornette, Didier (2021): Addressing insurance of data breach cyber risks in the catastrophe framework. In: *Geneva Pap Risk Insur Issues Pract* 46 (1), S. 53–78. DOI: 10.1057/s41288-020-00163-w.

Wolff, Josephine; Lehr, William (2017): Degrees of Ignorance About the Costs of Data Breaches: What Policymakers Can and Can't Do About the Lack of Good Empirical Data. Online verfügbar unter https://ssrn.com/abstract=2943867, zuletzt geprüft am 20.01.2021.

Wollinger, Gina Rosa; Dreißigacker, Arne; von Skarczinski, Bennet Simon (2020): Formen der Bedrohung von Cyberkriminalität. In: Gina Rosa Wollinger und Anna Schulze (Hg.): Handbuch Cybersecurity für die öffentliche Verwaltung. Wiesbaden: Kommunal- und Schul-Verlag (KSV Verwaltungspraxis), S. 27–56.

Woods, Daniel W.; Böhme, Rainer (2021): Systematization of Knowledge: Quantifying Cyber Risk. In: *42nd IEEE Symposium on Security and Privacy*.

Wrede, Dirk; Stegen, Tino; Schulenburg, Johann-Matthias Graf von der (2020): Affirmative and silent cyber coverage in traditional insurance policies: Qualitative content analysis of selected insurance products from the German insurance market. In: *Geneva Pap Risk Insur Issues Pract* 45 (4), S. 657–689. DOI: 10.1057/s41288-020-00183-6.

Teil B – Forschungsbeiträge

Beitrag A: Cyber-Dependent Crime Victimization: The Same Risk for Everyone?

Beitrag A	
Autoren und Autorinnen	Bergmann, Marie Christine; Dreißigacker, Arne; **von Skarczinski, Bennet**; Wollinger, Gina Rosa
Publikationsmedium	Journal
Publikationsorgan	Cyberpsychology, Behavior, and Social Networking (Mary Ann Liebert)
Jahr	2018
Ranking	**Q1** – SCImago Journal Rank Indicator (SJR): 1,466 [13] **Top 94 Perzentil** – Scopus CiteScore: 8,7 [14]
Status	Veröffentlicht
Bibliographische Informationen	Bergmann, Marie Christine; Dreißigacker, Arne; **von Skarczinski, Bennet Simon**; Wollinger, Gina Rosa (2018): Cyber-Dependent Crime Victimization: The Same Risk for Everyone? In: Cyberpsychology, behavior and social networking 21 (2), S. 84–90. DOI: 10.1089/cyber.2016.0727.
Identifikation	10.1089/cyber.2016.0727
Link	https://www.liebertpub.com/doi/abs/10.1089/cyber.2016.0727
Keywords	victimization, cybercrime, cyber-dependent crime, risk factor, routine activity

Abstract - The Internet has simplified daily life activities. However, besides its comfortability, the Internet also presents the risk of victimization by several kinds of crimes. The present article addresses the question of which factors influence cyber-dependent crime and how they vary between three kinds of cyber-dependent offences: malware infection, ransomware infection, and misuse of personal data. According to the Routine Activity Approach, it is assumed that crime is determined by a motivated offender, the behavior of the Internet user, and the existence of prevention factors. Our analyses were based on a random sample of 26,665 Internet users in two federal states in Germany, aged 16 years and older; 16.6 percent of the respondents had experienced at least one form of cyber-dependent victimization during the year 2014. The results indicate that individual and household factors, as well as online and prevention behavior, influence the risk of cyber-dependent victimization. Furthermore, the effects differ between the three types of offences. In conclusion, the risk of being victimized by cyber-dependent crime is not the same for anyone, but depends on multivariate factors according to the idea of Routine Activity Approach. However, in view of the fact that crime-related factors also matter, studying different cybercrime offences separately seems to be an appropriate research approach.

[13] Top 11,9% in Computer Science Journals; SJR = 1,466 (232 von 1956); Stand: 04.07.2023; https://www.scimagojr.com/journalrank.php?area=1700

[14] 94th percentile in Social Psychology Journals 2022; https://www.scopus.com/sourceid/19700176047

Beitrag B: A Large-Scale Interview Study on Information Security in and Attacks against Small and Medium-sized Enterprises

Beitrag B	
Autoren und Autorinnen	Huaman, Nicolas; **von Skarczinski, Bennet Simon**; Wermke, Dominik; Stransky, Christian; Acar, Yasemin; Dreißigacker, Arne; Fahl, Sascha
Publikationsmedium	Konferenz
Publikationsorgan	30th USENIX Security Symposium
Jahr	2021
Ranking	**A*** - CORE Ranking [15] **TIER 1** - TAMU [16]
Status	Veröffentlicht
Bibliographische Informationen	Huaman, Nicolas; **von Skarczinski, Bennet Simon**; Wermke, Dominik; Stransky, Christian; Acar, Yasemin; Dreißigacker, Arne; Fahl, Sascha (2021): A Large-Scale Interview Study on Information Security in and Attacks against Small and Medium-sized Enterprises. In: Proceedings of the 30th USENIX Security Symposium.
Identifikation	978-1-939133-24-3
Link	https://www.usenix.org/conference/usenixsecurity21/presentation/huaman
Keywords	-

Abstract - Cybercrime is on the rise. Attacks by hackers, organized crime and nation-state adversaries are an economic threat for companies world-wide. Small and medium-sized enterprises (SMEs) have increasingly become victims of cyberattacks in recent years. SMEs often lack the awareness and resources to deploy extensive information security measures. However, the health of SMEs is critical for society: For example, in Germany, 38.8% of all employees work in SMEs, which contributed 31.9% of the German annual gross domestic product in 2018. Many guidelines and recommendations encourage companies to invest more into their information security measures. However, there is a lack of understanding of the adoption of security measures in SMEs, their risk perception with regards to cybercrime and their experiences with cyberattacks. To address this gap in research, we performed 5,000 computer-assisted telephone-interviews (CATIs) with representatives of SMEs in Germany. We report on their experiences with cybercrime, management of information security and risk perception. We present and discuss empirical results of the adoption of both technical and organizational security measures and risk awareness in SMEs. We find that many technical security measures and basic awareness have been deployed in the majority of companies. We uncover differences in reporting cybercrime incidences for SMEs based on their industry sector, company size and security awareness. We conclude our work with a discussion of recommendations for future research, industry and policy makers.

[15] CORE Ranking 2021: A* - flagship conference, a leading venue in a discipline area (7.45% of 792 ranked venues); http://portal.core.edu.au/conf-ranks/?search=USenix&by=all&source=CORE2021&sort=atitle&page=1 (04.07.2023)

[16] Texas A&M University, Security Conference Ranking and Statistic (Annahmequote USENIX Security Symposum 2022: 18,1%); https://people.engr.tamu.edu/guofei/sec_conf_stat.htm (07.04.2023)

Beitrag C: Understanding the adoption of cyber insurance for residual risks - An empirical large-scale survey on organizational factors of the demand side

Beitrag C	
Autoren	**von Skarczinski, Bennet Simon**; Boll, Lukas; Teuteberg, Frank
Publikationsmedium	Konferenz
Publikationsorgan	European Conference in Information Systems (ECIS)
Jahr	2021
Ranking	**A** - WKWI **B** - VHB JQ3 **A** - VHB Rating 2024
Status	Veröffentlicht
Bibliographische Informationen	**von Skarczinski, Bennet Simon**; Boll, Lukas; Teuteberg, Frank (2021): Understanding the adoption of cyber insurance for residual risks - An empirical large-scale survey on organizational factors of the demand side. In: ECIS Proceedings (72). Online verfügbar unter https://aisel.aisnet.org/ecis2021_rp/72/.
Identifikation	-
Link	https://aisel.aisnet.org/ecis2021_rp/72/
Keywords	Cyber Insurance, IT-Security Investments, TOE Framework, Adoption of Information Security Measures

Abstract - This research paper analyzes technological, organizational, and environmental (TOE framework) adoption factors of cyber insurances (CI) by conducting a computer-assisted telephone interview study with 2,483 German firms. Considering our screening of related literature, this study, to our knowledge, is the first large-scale empirical study analyzing organizational adoption factors of CI on the demand side. We distinguish between firms that have or have not considered CI and those that have or have not adopted CI following considerations. Our regression results indicate that there are statistically significant factors on the consideration and adoption of CI across all TOE dimensions. Subsequently, we discuss the extent to which CI is perceived as an appropriate tool to manage information security and derive propositions for the education of firms and further research in academia.

Beitrag D: Toward enhancing the information base on costs of cyber incidents: implications from literature and a large-scale survey conducted in Germany

Beitrag D	
Autoren	**von Skarczinski, Bennet Simon**; Dreißigacker, Arne; Teuteberg, Frank
Publikationsmedium	Journal
Publikationsorgan	Organizational Cybersecurity Journal: Practice, Process and People (Emerald)
Jahr	2022
Ranking	Kein Ranking / Score verfügbar[17]
Status	Veröffentlicht
Bibliographische Informationen	**von Skarczinski, Bennet Simon**; Dreißigacker, Arne; Teuteberg, Frank (2022): Toward enhancing the information base on costs of cyber incidents: implications from literature and a large-scale survey conducted in Germany. In: OCJ. DOI: 10.1108/OCJ-08-2021-0020.
Identifikation	https://doi.org/10.1108/OCJ-08-2021-0020
Link	https://www.emerald.com/insight/content/doi/10.1108/OCJ-08-2021-0020/full/html
Keywords	Impact of data breaches, Management of information security, IT-security investments, Cost-benefit benchmark, Cyber losses

Abstract

Purpose – Literature repeatedly complains about the lack of empirical data on the costs of cyber incidents within organizations. Simultaneously, managers urgently require transparent and reliable data in order to make well-informed and cost-benefit optimized decisions. The purpose of this paper is to (1) provide managers with differentiated empirical data on costs, and (2) derive an activity plan for organizations, the government and academia to improve the information base on the costs of cyber incidents. **Design/ methodology/ approach –** The authors analyze the benchmark potential of costs within existing literature and conduct a large-scale interview survey with 5,000 German organizations. These costs are directly assignable to the most severe incident within the last 12 months, further categorized into attack types, cost items, employee classes and industry types. Based on previous literature, expert interviews and the empirical results, the authors draft an activity plan containing further research questions and action items. **Findings –** The findings indicate that the majority of organizations suffer little to no costs, whereas only a small proportion suffers high costs. However, organizations are not affected equally since prevalence rates and costs according to attack types, employee classes, and other variables tend to vary. Moreover, the

[17] Für das Publikationsorgan des Beitrages D liegen derzeit noch keine Rankings vor, was daran liegen dürfte, dass das Organizational Cybersecurity Journal (OCJ) neugegründet wurde und die Erstausgabe 2021 erschien. Das OCJ erscheint im renommierten Emerald Verlag und wird von bekannten Indexing Services gelistet (z.B. EBSCO Discovery, Google Scholar, WorldCat). Die Universität von Colorado (USA) - Colorado Springs College of Business and Cybersecurity Management Council sponsort das OCJ, welches von Prof. Dr. Gurvirender Tejay als Editor-in-Chief geleitet wird. Die Gutachter und Gutachterinnen des OCJ stammen überwiegend von renommierten Universitäten aus den Vereinigten Staaten von Amerika (Emerald Publishing 2023), darunter auch die Senior Editors Prof. Dr. John D'Arcy, University of Delaware, und Prof. Dr. Mikko Siponen - University of Jyväskylä, Finnland, die selbst zahlreiche Beiträge in VHB JQ3 A-gerankten Publikationsorganen veröffentlicht haben (z.B. MIS Quarterly, European Journal of Information Systems (EJIS), Information Systems Research (ISR)).

findings indicate that board members and IS/IT-managers show partly different response behaviors. **Originality/value –** The authors present differentiated insights into the direct costs of cyber incidents, based on the authors' knowledge, this is the largest empirical survey in continental Europe and one of the first surveys providing in-depth cost information on German organizations.

Beitrag E: More Security, less Harm? Exploring the Link between Security Measures and Direct Costs of Cyber Incidents within Firms using PLS-PM

Beitrag E	
Autoren	**von Skarczinski, Bennet Simon**; Dreißigacker, Arne; Teuteberg, Frank
Publikationsmedium	Konferenz
Publikationsorgan	Wirtschaftsinformatik (WI)
Jahr	2022
Ranking	**A** - WKWI **C** -VHB JQ3 **B** - VHB Rating 2024
Status	Veröffentlicht
Bibliographische Informationen	**von Skarczinski, Bennet Simon**; Dreissigacker, Arne; Teuteberg, Frank (2022): More Security, less Harm? Exploring the Link between Security Measures and Direct Costs of Cyber Incidents within Firms using PLS-PM. In: Wirtschaftsinformatik 2022 Proceedings (2).
Identifikation	-
Link	https://aisel.aisnet.org/wi2022/it_strategy/it_strategy/2
Keywords	IT-security investment, cybercrime losses, impact of data breaches

Abstract - As one of the first articles to empirically explore the direct costs of cyber incidents, our research provides novel and significant insights into the structural links between cyber incidents, exposure, and security within firms, as well as the related technical consequences. We employ an explorative approach, which is based on the causal information/cyber risk models proposed by Cohen et al. and Woods & Böhme, as well as PLS-modeling to analyze data from 493 firms that have incurred direct costs from their most severe cyber incident in the last 12 months. These data are part of a larger dataset, based on a representative and stratified random sample of 5,000 organizations that participated in a survey in 2018/19. Based on our model, we discuss the results and derive implications that are highly relevant to the alignment of IT (security) strategy and management. Furthermore, we identify gaps to be assessed in future research.

Beitrag F: Modelling maximum cyber incident losses of German organisations: an empirical study and modified extreme value distribution approach

Beitrag F	
Autoren	**von Skarczinski, Bennet Simon**; Raschke, Mathias; Teuteberg, Frank
Publikationsmedium	Journal
Publikationsorgan	The Geneva Papers on Risk and Insurance - Issues and Practice (Palgrave Macmillan / Springer Nature)
Jahr	2023
Ranking	**B** - VHB JQ3 **B** - VHB Rating 2024
Status	Veröffentlicht
Bibliographische Informationen	**Skarczinski, Bennet von**; Raschke, Mathias; Teuteberg, Frank (2023): Modelling maximum cyber incident losses of German organisations: an empirical study and modified extreme value distribution approach. In: Geneva Pap Risk Insur Issues Pract 48 (2), S. 463–501. DOI: 10.1057/s41288-023-00293-x
Identifikation	DOI: 10.1057/s41288-023-00293-x
Link	https://link.springer.com/article/10.1057/s41288-023-00293-x
Keywords	Cyber incident losses · Loss size distribution · Extreme value distribution · Tapered distribution · Information security management · Data breach

Abstract - Cyber incidents are among the most critical business risks for organisations and can lead to large financial losses. However, previous research on loss modelling is based on unassured data sources because the representativeness and completeness of oprisk databases cannot be assured. Moreover, there is a lack of modelling approaches that focus on the tail behaviour and adequately account for extreme losses. In this paper, we introduce a novel 'tempered' generalised extreme value (GEV) approach. Based on a stratified random sample of 5000 interviewed German organisations, we model different loss distributions and compare them to our empirical data using graphical analysis and goodness-of-fit tests. We differentiate various subsamples (industry, size, attack type, loss type) and find our modified GEV outperforms other distributions, such as the lognormal and Weibull distributions. Finally, we calculate losses for the German economy, present application examples, derive implications as well as discuss the comparison of loss estimates in the literature.