TECHNISCHE UNIVERSITÄT DARMSTADT

Cyberrisiken – Drei Studien über deren Begrifflichkeit, Quantifizierung und Risikomanagement

vom Fachbereich Rechts- und Wirtschaftswissenschaften der Technischen Universität Darmstadt

zur Erlangung des akademischen Grades
Doctor rerum politicarum
(Dr. rer. pol.)

Dissertation
von Daniel Zängerle

Erstgutachter: Prof. Dr. Dirk Schiereck
Zweitgutachter: Prof. Dr. Peter Buxmann

Darmstadt 2023

Zängerle, Daniel: Cyberrisiken – Drei Studien über deren Begrifflichkeit, Quantifizierung und Risikomanagement
Darmstadt, Technische Universität Darmstadt,
Jahr der Veröffentlichung der Dissertation auf TUprints: 2023
URN: urn:nbn:de:tuda-tuprints-243851
Tag der mündlichen Prüfung: 07.07.2023

Vorwort

Die vorliegende Dissertation wäre ohne die Unterstützung vieler wunderbarer Menschen nicht möglich gewesen. Ihnen alle möchte ich an dieser Stelle von Herzen danken.

Herzlichen Dank, lieber Prof. Dr. Dirk Schiereck, für die kontinuierliche und engagierte Betreuung meines Promotionsvorhabens. Danke für das stets übermittelte Vertrauen, die zahlreichen Impulse und gewährten inhaltlichen Freiräume in der Erarbeitung dieser Dissertation.

Herzlichen Dank, lieber Prof. Dr. Buxmann, für die Übernahme des Zweitgutachtens meiner Dissertationsschrift sowie die fachkritischen Anmerkungen und Diskussionen.

Vielen Dank an den VÖB-Service und Petra Ludwig für die konstruktive Zusammenarbeit und die Bereitstellung der ÖffSchOR-Datenbank im Rahmen dieses Dissertationsvorhabens.

Vielen Dank an die Deutsche Gesellschaft für Operational Risk Management e.V. für den fachlichen Austausch und die zahlreichen Hinweise und Anregungen, die diese Dissertation bereichert haben.

Vielen Dank an alle Cybersicherheitsexpertinnen und -experten für die unzensierten und transparenten Einblicke, die den dritten Forschungsbeitrag ermöglicht haben. Ein besonderer Dank an die CISO-Runde der Universitätskliniken Deutschlands, die das Forschungsvorhaben umfassend unterstützt und beworben haben.

Vielen Dank an die Roland Berger GmbH, Dr. Christian Krys und Dr.-Ing. Martin Streichfuss, die sowohl die finanzielle als auch die organisatorische Unterstützung zur Durchführung dieses Promotionsvorhabens ermöglichten. Danke an Dr. Johannes Klein, der mich zu dieser akademischen Weiterentwicklung ermutigte. Herzlichen Dank an alle Kolleginnen und Kollegen des Roland Berger Doktorandenprogramms, insbesondere Leonie, Louisa und Manuel, für die wertvollen Diskussionen, konstruktiven Anregungen und stets unterstützende Attitüde.

Mein größter Dank gilt meiner Frau Chloé, die mich an guten, wie an weniger guten Tagen begleitet und mich stets aufs Neue motiviert. Vielen Dank für deine verständnisvolle Art und deine unermüdliche Unterstützung vor, während und nach dieser Promotion.

Abschließend möchte ich herzlichst meinen Eltern danken, die mir diesen Bildungsweg initial ermöglicht haben. Als First Generation Studierender bin ich besonders stolz, dass ihr allzeit an mich geglaubt sowie mich bekräftigt habt, meinen eigenen Weg im Leben zu gehen.

Düsseldorf, im April 2023 Daniel Zängerle

Für Ida

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

AIC*	Akaike information criterion
AUC*	Area under curve
B3S*	Branchenspezifischer Sicherheitsstandard
BCM*	Business continuity management
Bill.*	Billionen
BKA	Bundeskriminalamt
BSI	Bundesamt für Sicherheit in der Informationstechnik
CDO*	Chief Digital Officer
CEO*	Chief Executive Officer
CIO*	Chief Information Officer
CISO*	Chief Information Security Officer
Clusit*	Associazione Italiana per la Sicurezza Informatica
CMIO*	Chief Medical Information Officer
CRO*	Chief Risk Officer
CRR*	Capital Requirements Regulation
CURF*	Core unified risk framework
DACH*	Deutschland (D), Österreich (A) und die Schweiz (CH)
DakOR*	Datenkonsortium OpRisk
DDoS*	Distributed Denial of Service
DIPO*	Italian Database of Operational Losses
DRG*	Diagnosis related groups
ERM*	Enterprise risk management
EVT*	Extreme value theory
GDPR*	General Data Protection Regulation
GPD*	Generalised pareto distribution
HLT*	Hosmer–Lemeshow test
ICT*	Information and communication technology
IDS*	Intrusion detection system
IFM*	Inference functions for margins
IKT*	Informations- und Kommunikationstechnologie
IoT*	Internet of Things
IS	Informationssicherheit
ISB*	Informationssicherheitsbeauftragte(r)
ISM*	Informationssicherheitsmanagement

Hinweis: Abkürzungen mit der Kennzeichnung * sind in den Forschungsbeiträgen 1 bis 3 enthalten.

ISMS	Informationssicherheitsmanagementsystem (*Englisch: Information security management system*)
ISO	International Organisation for Standardization
ISRA*	Information security risk assessment
IT	Informationstechnologie
KHZF*	Krankenhauszukunftsfonds
KHZG*	Krankenhauszukunftsgesetz
KI*	Künstliche Intelligenz
KRITIS	Kritische Infrastruktur
LL*	Log-likelihood
MAE*	Mean absolute error
MLE*	Maximum likelihood estimation
MSE*	Mean standard error
NGS*	Next generation sequencing
NIST	National Institute of Standards and Technology
OCTAVE*	Operationally critical threat, asset, and vulnerability evaluation
ÖffSchOR	Öffentliche Schadenfälle OpRisk
OpRisk	Operationelle Risiken
ORX*	Operational Riskdata eXchange Association
OT*	Operational technology
PCC*	Pairwise copula construction
POT*	Peaks-over-threshold
PRC*	Privacy Rights Clearinghouse
QBowTie*	Quantitative Bow-tie
RPS*	Ranked probability score
SD*	Standard deviation
SIEM*	Security information and event management
SOC*	Security operation centre
TVaR*	Tail value at risk
VaR*	Value at risk
VERIS*	Vocabulary for Event Recording and Incident Sharing
VÖB*	Bundesverband Öffentlicher Banken Deutschlands
WEF*	World Economic Forum
WRIEC*	World Risk and Insurance Economics Conference
z.B.*	zum Beispiel

Hinweis: Abkürzungen mit der Kennzeichnung * sind in den Forschungsbeiträgen 1 bis 3 enthalten.

1 Synopse

In diesem Kapitel besteht die Zielsetzung darin, eine Einführung in Bezug auf das Forschungsvorhaben und dessen Einordnung in die Literatur zu geben. Zunächst werden Motivation und Relevanz des Forschungsbereichs ‚Cyberrisiken' erläutert (Unterkapitel 1.1). Anschließend werden konkrete Forschungsfragen hergeleitet und deren Einordnung in einen konzeptionellen Gesamtrahmen wird vorgestellt (Unterkapitel 1.2). Danach werden die Struktur der Dissertationsschrift sowie die Kerninhalte der drei empirischen Studien dieser Abhandlung präsentiert (Unterkapitel 1.3).

1.1 Motivation und Hintergrund

Die Welt des 21. Jahrhunderts ist einer Vielzahl globaler Großrisiken ausgesetzt. Neben sozialen, geopolitischen und ökologischen Herausforderungen zählen Cyberkriminalität und die Gefährdung der Cybersicherheit zu den größten Bedrohungen des Jahrzehnts (World Economic Forum, 2023). Cyberrisiken bedrohen nicht nur die Vertraulichkeit, Verfügbarkeit und Integrität von Informationen, sondern können auch zu hohen finanziellen Vermögensschäden, Betriebsunterbrechungen, Datendiebstahl und Reputationsverlusten führen (Cavusoglu et al., 2004; Smith, 2004; Salmela, 2008; Bulgurcu et al., 2010; Innerhofer-Oberperfler & Breu, 2010; Järveläinen, 2013; Wrede et al., 2018). Mit der Verbreitung des Internets und der stetig voranschreitenden Digitalisierung haben sowohl die Häufigkeit und Komplexität als auch das Ausmaß von Cyberrisiken stark zugenommen (Njegomir & Marović, 2012; Eling & Wirfs, 2019). Dies geht auch aus dem aktuellen Lagebericht zur Cybersicherheit des Bundesamts für Sicherheit in der Informationstechnik (BSI) hervor, das vor einer weiteren Anspannung der Bedrohungslage durch Cyberkrieg und die Professionalisierung der Angreifer warnt (Bundesamt für Sicherheit in der Informationstechnik, 2022). Gemäß Abbildung 1-1 werden die weltweiten Kosten der Cyberkriminalität im Jahr 2022 auf mehr als acht Billionen Euro geschätzt, während bis zum Jahr 2027 eine Verdreifachung der jährlichen Schadenssumme auf circa 23,8 Billionen Euro erwartet wird (Statista, 2022). Allein in Deutschland werden die finanziellen Auswirkungen von Cyberangriffen auf mehr als 200 Milliarden Euro beziffert (Bitkom, 2022). Zudem werden bundesweit mehr als 108.000 Fälle von Cyberkriminalität durch das Bundeskriminalamt (BKA) und damit doppelt so viele Fälle wie noch im Jahr 2015 registriert (Bundeskriminalamt, 2021). Die enormen Gefahrenpotenziale von Cyberrisiken betreffen heutzutage nicht nur private Internetnutzer, sondern stellen vor allem Unternehmen und Organisationen aller Größenordnungen sowohl im öffentlichen als auch privaten Sektor vor neue Herausforderungen (Njegomir & Marović, 2012; Choudhry, 2014; Bendovschi, 2015; Wrede et al., 2018; Aldasoro et al., 2020). Dessen ungeachtet verschärft sich aufgrund der

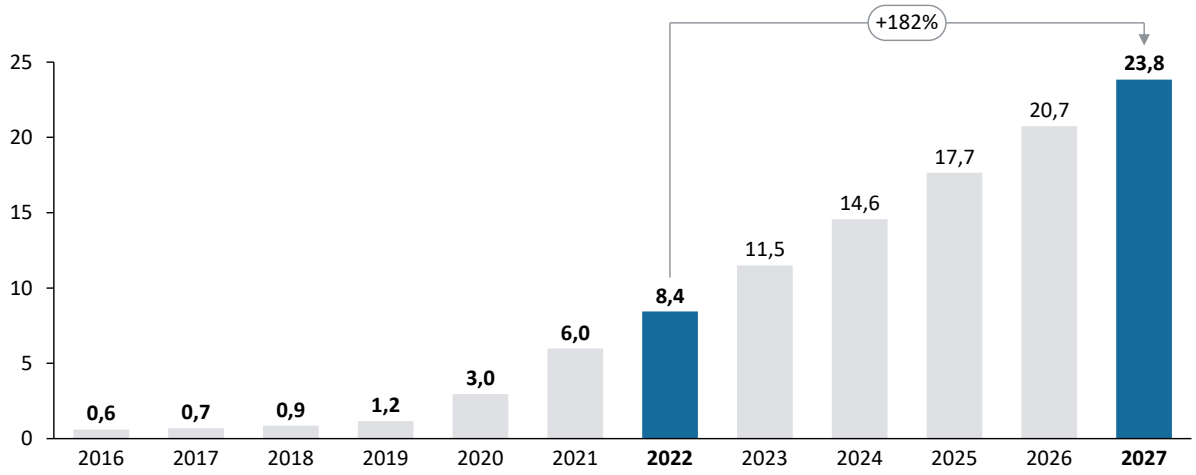

Abbildung 1-1: Geschätzte Kosten der weltweiten Cyberkriminalität von 2016 bis 2027 [in Bill. EUR]
Quelle: Statista (2022), Zugriff am 26.01.2023

weltweiten Vernetzung der Informationstechnologie (IT) und der Nutzung von IT-Produkten und -Dienstleistungen die existenzielle Bedrohungslage durch Cyberrisiken (Rakes et al., 2012; Aldasoro et al., 2020). Selbst Cyberereignisse ohne gravierende wirtschaftliche Auswirkungen können sich für ein einzelnes Unternehmen als existenzbedrohend in Form finanzieller Schäden oder von Image- und Reputationsverlusten erweisen (Cavusoglu et al., 2004; Wrede et al., 2018; Kamiya et al., 2021).

Der im Mai 2020 erfolgte Cyberangriff auf die Betreiber von Colonial Pipelines illustriert, welchen Einfluss und welche weitreichenden Auswirkungen Cyberrisiken nehmen können (Handelsblatt, 2021). Aufgrund eines kriminellen Angriffs der Hackergruppe ‚Darkside' hat das Unternehmen bestimmte Systeme vom Netz genommen, wodurch der Betrieb der Benzin-Pipeline für mehrere Tage zum Erliegen kam und Engpässe in Teilen der Vereinigten Staaten bedingte. Beispielsweise war an 70 Prozent der Tankstellen in North Carolina kein Benzin mehr erhältlich, und der Ölpreis sank an den Börsen um fast einen US-Dollar pro Barrel. Zudem forderten die Hacker ein Lösegeld in Höhe von fast fünf Millionen US-Dollar zur Entschlüsselung der außer Betrieb gesetzten Systeme. Dieser Forderung kam Colonial nur wenige Stunden nach der Attacke nach, benötigte jedoch mehrere Tage, um den Betrieb wieder vollständig aufzunehmen. Weitere noch nicht berücksichtigte Auswirkungen in diesem Fallbeispiel sind unter anderem die tatsächlichen Wiederherstellungs- und erforderlichen Aufrüstungskosten der Systeme sowie der IT-Sicherheit, mögliche Rechts- und Haftungskosten sowie eine im Nachgang zu erwartende Erhöhung der Versicherungsprämie.

Solche schwerwiegenden Cybervorfälle sind keine Seltenheit, sondern ereignen sich ebenso in Deutschland, wie die jüngsten Vorfälle am Lukaskrankenhaus Neuss (Argaw et al., 2020), am Universitätsklinikum Düsseldorf (Kucera, 2020) oder beim Automobilzulieferer Continental

(Continental, 2023) beweisen. Cyberrisiken können überall entstehen – sie folgen keinen (Länder-)Grenzen oder Regeln und gelten als opak (Smidt & Botzen, 2018).

Infolgedessen liegt die Vermutung nahe, dass der Schutz vor Cyberrisiken und die Cybersicherheit im Allgemeinen von höchster Priorität für die Wirtschaft sind und zunehmend an strategischer Bedeutung für Unternehmen sowie deren Management gewinnen (Gordon & Loeb, 2002; Kayworth & Whitten, 2012; Kruger & Kearney, 2006; Solms & Niekerk, 2013; Sonnenreich et al., 2006; Wrede et al., 2018). Das notwendige Bewusstsein, die sogenannte Cyber Security Awareness, ist in der Praxis jedoch nicht vollständig entwickelt, wie in Abbildung 1-2 illustrativ dargestellt. In einer repräsentativen Umfrage des Rückversicherers Munich Re (2022) haben Vorstände in Schweden (42 %), Norwegen (42 %) und Deutschland (58 %) eine im Schnitt deutlich geringere Cyber Security Awareness im Vergleich zu brasilianischen (89 %), australischen (76 %) und französischen (76 %) Vorständen. Daher zählt die Schaffung eines ausgeprägten Risikobewusstseins in Bezug auf Cybersicherheit – insbesondere in Deutschland – zu den bedeutendsten Aufgaben des IT- und Informationssicherheitsmanagements (Thomson & Solms, 1998; Nosworthy, 2000; Kritzinger & Smith, 2008; Tsohou et al., 2012; Abawajy, 2014; Wrede et al., 2018).

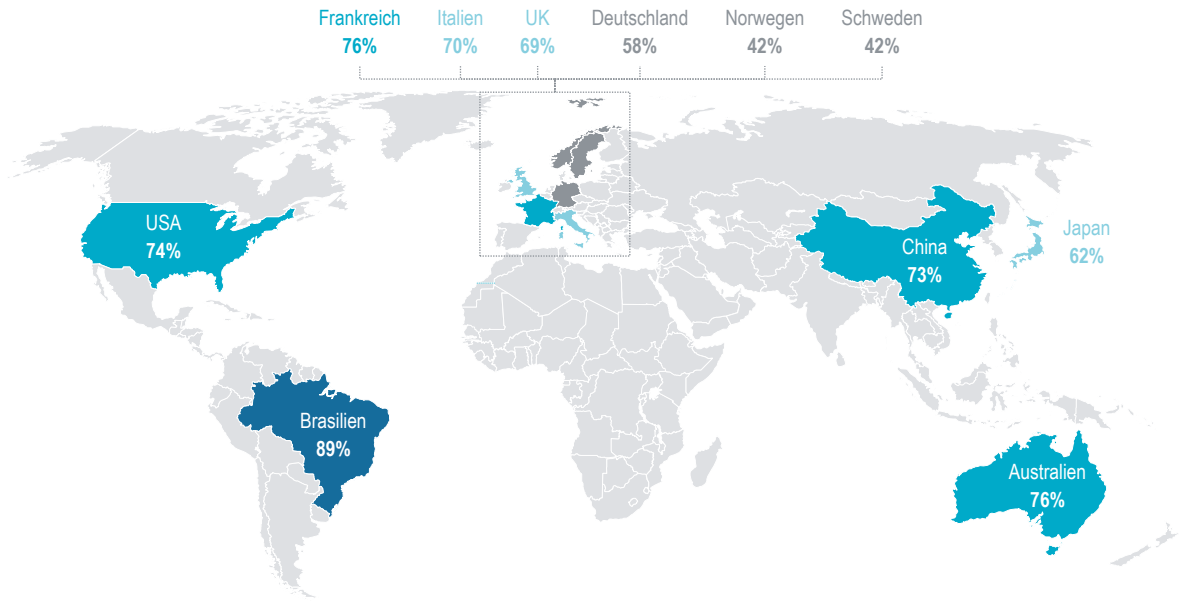

Abbildung 1-2: Cyber Security Awareness befragter Vorstände aus ausgewählten Ländern

Anmerkung: Wie sehr befürchten Sie einen möglichen Cyberangriff auf Ihr Unternehmen? Beispielsweise sind mehr als 8 von 10 Befragten in Brasilien besorgt oder äußerst besorgt über einen Cyberangriff. Quelle: Munich Re (2022). Zugriff am 28.01.2023

Die wissenschaftliche und praxisnahe Forschung zum Thema Cyberrisiko hat in den vergangenen Jahren gleichsam zugenommen. Allerdings befindet sich das Forschungsfeld noch in den Anfängen und ist durch interdisziplinäre Barrieren beschränkt (Falco et al., 2019b). Trotz der zunehmenden Relevanz von Cyberrisiken in zahlreichen wissenschaftlichen Disziplinen hat das

Thema in der wirtschafts- und versicherungswissenschaftlichen Literatur bisher kaum Beachtung gefunden (Eling, 2020), was einen Grund für die unerwartet niedrige Awareness verkörpert.

Vor diesem Hintergrund wird mit der vorliegenden Dissertation das Ziel verfolgt, das Thema Cyberrisiko unter verschiedenen wirtschafts- und versicherungswissenschaftlichen Blickwinkeln zu beleuchten, um das Verständnis und das Bewusstsein für Cyberrisiken in Wissenschaft und Praxis zu verbessern. Aufgrund der Komplexität und Multidisziplinarität der Cyberrisikoforschung ist sowohl die Formulierung als auch die Beantwortung einer einzigen übergreifenden Forschungsfrage nicht möglich, weshalb im folgenden Unterkapitel – basierend auf der wissenschaftlichen Literatur – die genauen Forschungsfragen formuliert und im Rahmen von drei dedizierten Forschungsbeiträgen beantwortet werden.

1.2 Forschungsfragen und literarische Einbettung

Über das vergangene Jahrzehnt hat sowohl die wissenschaftliche als auch praxisnahe Forschung zum Thema Cyberrisiko stark an Bedeutung gewonnen. Dies spiegelt sich beispielsweise in der kontinuierlich steigenden Anzahl an Veröffentlichungen wider, unter anderem in der Informatik, im Ingenieurwesen sowie der Betriebswirtschaft und den Wirtschafts- und Sozialwissenschaften (Eling, 2020). Zudem findet sich das Thema Cyberrisiko auf immer mehr Tagesordnungen und Podiumsdiskussionen führender Konferenzen, zum Beispiel auf der World Risk and Insurance Economics Conference (WRIEC) 2020 (Boyer, 2020).[1] Jedoch geht jedes Fachgebiet davon aus, das Thema Cyberrisiko umfassend zu behandeln, auch wenn es an holistischen Ansätzen und disziplinübergreifender Forschung fehlt (Falco et al., 2019b). Vor diesem Hintergrund sowie der erforderlichen Zusammenarbeit und Vernetzung unterschiedlicher forschungs- und praxisnaher Experten in der Zukunft hat eine Gruppe führender Wissenschaftler, Branchenexperten und politischer Vertreter aus aller Welt eine umfassende Forschungsagenda mit sechs Grundsatzfragen (vgl. Abbildung 1-3) erarbeitet, die der Vielfalt an relevanten Fragestellungen zum Thema Cyberrisiko gerecht werden soll (Falco et al., 2019a). Das in Abbildung 1-3 dargestellte Konzeptmodell dient mithin als Ausgangsbasis dieser Dissertation, wobei sich jeder Forschungsbeitrag auf ein bestimmtes Thema der postulierten Grundfragen konzentriert. Dementsprechend liefert diese Dissertation einen wissenschaftlichen Beitrag zur Beantwortung von drei der insgesamt sechs Grundsatzfragen. Im Folgenden werden die konkreten Forschungsfragen hergeleitet und in die Forschungsagenda von Falco et al. (2019a) eingeordnet.

[1] Im Rahmen der WRIEC 2020 wurde erstmalig eine dedizierte Sitzung zum Thema Cyberrisiko abgehalten (https://www.wriec2020.org).

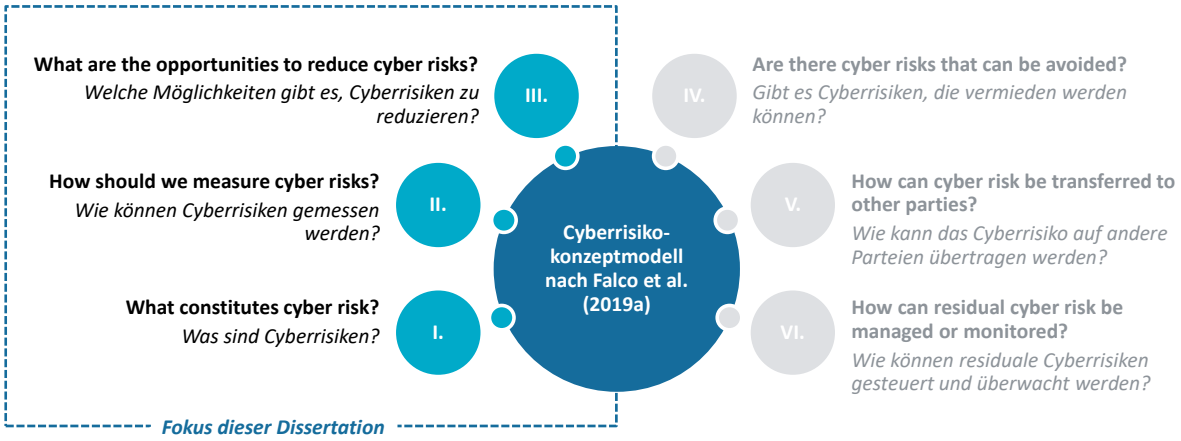

Abbildung 1-3: Cyberrisiko-Konzeptmodell nach Falco et al. (2019a) (eigene Darstellung)

1.2.1 Was sind Cyberrisiken?

Cyberrisiken sind vielfältig und umfassen ein ganzes Spektrum von Angriffsformaten, denen Unternehmen ausgesetzt sind. Diese reichen von unbeabsichtigten Datenlecks über böswillige Versuche, digitale Systeme zu beschädigen oder vertrauliche Unternehmensdaten zu stehlen, bis hin zu strategischen Cyberangriffen durch Wettbewerber oder politische Institutionen. Das Ausmaß eines Cybervorfalls lässt sich nur schwierig charakterisieren, da über die Bedeutung eines Cyberereignisses weiterhin Uneinigkeit besteht. Vor allem in der internen Unternehmensbetrachtung ist es erforderlich, dass alle Mitarbeiter – vom Topmanagement bis hin zu den Angestellten – ein gleiches Begriffsverständnis erfahren, um für das Thema Cyberrisiko sensibilisiert zu werden und sich während eines Vorfalls adäquat zu verhalten. Gleichwohl ist bislang kein einheitliches Begriffsverständnis vorhanden – sowohl in der Praxis als auch in der wissenschaftlichen und praxisnahen Literatur. Selbst führende Standardisierungsorganisationen wie das National Institute of Standards and Technology (NIST) oder die International Organisation for Standardization (ISO) nutzen unterschiedliche Definitionsansätze des Terminus Cyberrisiko. Diesem Aspekt ist es geschuldet, dass es an einem übergreifenden Begriffskonstrukt (Eling, 2018) sowie einer eindeutigen Abgrenzung zu verwandten Begrifflichkeiten mangelt, zum Beispiel in Bezug auf IT- und Informationssicherheit (IS). Für die weitere Cyberforschung ist eine klare und einheitliche Cyberterminologie unerlässlich. Unterschiedliche Definitionen eines Cyberrisikos schränken die Möglichkeiten einer einheitlichen Berichterstattung und Datenanalyse über Cyberrisiken ein. Außerdem wird der wissenschaftliche Fortschritt durch die dargelegte uneinheitliche Nutzung der Terminologie erschwert und sogar eingeschränkt.

(1a) *Wie ist der Terminus ‚Cyberrisiko' in der wissenschaftlichen Literatur definiert?*

(1b) *Inwiefern lässt sich der Terminus ‚Cyberrisiko' von verwandten Begrifflichkeiten formal abgrenzen?*

1.2.2 Wie können Cyberrisiken gemessen werden?

Zur Schaffung eines gemeinsamen Verständnisses über die Cybersicherheitslage eines Unternehmens bedarf es einheitlicher Kennzahlen, mit denen das Ausmaß von Cyberrisiken für interne und externe Zwecke festgelegt werden kann. Beispielsweise sind solche Maßzahlen für die Bewilligung von Cybersicherheitsbudgets sowie für das interne Risikomanagement erforderlich. Allerdings zeigt sich, dass bisherige Cyberrisiko-Managementansätze im Allgemeinen qualitativ und quantitativ unzureichend sind (Palsson et al., 2020). Die übliche Methode zur Quantifizierung von (Cyber-)Risiken besteht in der Analyse historischer Schadensereignisse aus verifizierbaren Quellen und der Durchführung empirischer, statistischer und versicherungsmathematischer Untersuchungen, um die finanziellen Auswirkungen und die Wahrscheinlichkeit eines Cybervorfalls in einer bestimmten Organisation zu bestimmen (Smidt & Botzen, 2018; Palsson et al., 2020). Trotz öffentlicher und privater Initiativen zum Aufbau von Cyberdatenbanken haben die Unternehmen wenig Anreiz, vertrauliche Informationen zu internen Cybervorfällen in einer öffentlichen oder konsortialen Datenbank zu teilen (Palsson et al., 2020). Der Mangel an historischen Daten schränkt indes die Qualität der Risikobewertungen ein und untergräbt die vielen Bemühungen von Unternehmen, Versicherern und der Politik, ein effektiveres Cyberrisikomanagement zu etablieren (Eling & Schnell, 2016; Marotta et al., 2017; Romanosky et al., 2019; Cremer et al., 2022).

Dessen ungeachtet erfassen die aktuellen Modelle nicht die beträchtlichen gegenseitigen Abhängigkeiten zwischen digitalisierten Systemen und ihren jeweiligen Branchen. Der Ausfall oder die Kompromittierung eines einzelnen digitalen Systems kann zu kaskadenartigen Ausfällen und exponentiellen Auswirkungen führen. Dies erschwert die Kalkulation des Cyberrisikos eines Unternehmens. Es ist unklar, wo die Grenze gezogen werden soll, an der das Cyberrisiko eines Unternehmens endet und das eines anderen beginnt.

Mithin sind Methoden vonnöten, um die Modellierung von voneinander abhängigen Cybereregnissen zu verbessern und um Unternehmen besser auf Cyberbedrohungen in einer bestimmten Branche oder in mehreren voneinander abhängigen Branchen vorbereiten zu können. Darüber hinaus können solche Modelle helfen, das kumulierte Risikopotenzial zu bewerten. Dieser Forschungsbereich ist insbesondere für Anbieter von Cyberversicherungen relevant, um die Risikoexposition der Portfolios besser einschätzen und Risikotoleranzen definieren zu können.

(2a) *Wie und in welchem Umfang können Cyberereignisse modelliert und letztlich vorhergesagt werden?*

(2b) *Inwiefern existieren Unterschiede hinsichtlich der Eintrittswahrscheinlichkeit und des Ausmaßes von Cyberereignissen über (Sub-)Industrien hinweg?*

1.2.3 Welche Möglichkeiten gibt es, Cyberrisiken zu reduzieren?

Unternehmen erkennen zunehmend, dass sie sich nicht vollumfänglich vor allen Cyberbedrohungen schützen und diese abwehren können. Daraus resultiert die Notwendigkeit, die Sicherheit ihrer Systeme, Netzwerke und Daten nach Prioritäten zu ordnen und die Möglichkeiten zur Verringerung des Cyberrisikos über das gesamte Spektrum hinweg zu bewerten. Unternehmen verfügen jedoch lediglich über begrenzte Ressourcen zur Bewältigung von Cyberbedrohungen, während sich die regulatorischen Anforderungen an Datenschutz und Informationssicherheit in den vergangenen Jahren weiter verschärft haben. Besonders herausfordernd stellt sich die Situation im Gesundheitswesen als Teil der Kritischen Infrastruktur (KRITIS) dar. Zwar hat das Gesundheitswesen speziell von der Digitalisierung profitiert, allerdings ergeben sich neuartige Gefahren aus dem Cyberraum, die mit entsprechenden Cybersicherheitsmaßnahmen reduziert werden müssen (Pohlmann, 2019). Vor dem Hintergrund der jahrelangen Unterfinanzierung von Krankenhäusern (Schmitz & Pedell, 2013) und dem Mangel an wissenschaftlichen Erkenntnissen über die Cybersicherheitslage des Gesundheitswesens (Sardi et al., 2020) bedarf es empirisch fundierter Einblicke in den aktuellen Status quo und die Herausforderungen zur langfristigen Sicherstellung der Cybersicherheit im Gesundheitswesen.

(3a) *Wie gestaltet sich die Cybersicherheit in deutschen Krankenhäusern?*

(3b) *Welche Herausforderungen und Implikationen ergeben sich in der Zukunft zur Sicherstellung der Cybersicherheit im Gesundheitswesen?*

Zusammenfassend sind in Tabelle 1-1 die Forschungsfragen der Dissertation und deren Einordnung in die disziplinübergreifende Forschungsagenda von Falco et al. (2019a) veranschaulicht.

	Forschungsfragen der Dissertation	Einordnung gemäß des Cyberrisiko-Konzeptmodells von Falco et al. (2019a)	Studie
(1a)	Wie ist der Terminus ‚Cyberrisiko' in der wissenschaftlichen Literatur definiert?	***I.*** *What constitutes cyber risks?*	Studie 1
(1b)	Inwiefern lässt sich der Terminus ‚Cyberrisiko' von verwandten Begrifflichkeiten formal abgrenzen?	***I.*** *What constitutes cyber risks?*	Studie 1
(2a)	Wie und in welchem Umfang können Cyberereignisse modelliert und vorhergesagt werden?	***II.*** *How should we measure cyber risks?*	Studie 2
(2b)	Inwiefern existieren Unterschiede hinsichtlich der Eintrittswahrscheinlichkeit und des Ausmaßes von Cyberereignissen über (Sub-)Industrien hinweg?	***II.*** *How should we measure cyber risks?*	Studie 2
(3a)	Wie gestaltet sich die Cybersicherheit in deutschen Krankenhäusern?	***III.*** *What are the opportunities to reduce cyber risk?*	Studie 3
(3b)	Welche Herausforderungen und Implikationen ergeben sich in der Zukunft zur Sicherstellung der Cybersicherheit im Gesundheitswesen?	***III.*** *What are the opportunities to reduce cyber risk?*	Studie 3

Tabelle 1-1: Adressierte Forschungsfragen und Einordnung in die Literatur

1.3 Forschungsdesign und Struktur der Dissertation

Zur Beantwortung des im vorhergehenden Unterkapitels postulierten Forschungsfragen werden drei umfassende Forschungsbeiträge erarbeitet und in dieser Dissertationsschrift in einen konzeptionellen Rahmen eingeordnet. Der Aufbau der vorliegenden Arbeit ist Abbildung 1-4 zu entnehmen und wird im Folgenden kurz erläutert. Abschließend werden in Tabelle 1-2 die drei Forschungsbeiträge zusammengefasst.

Zu Beginn setzt die Synopse einen einführenden konzeptionellen Rahmen für das Forschungsvorhaben. Dabei wird in Unterkapitel 1.1 die zugrunde liegende Motivation für das Forschungsthema präsentiert und in Unterkapitel 1.2 in konkrete Forschungsfragen überführt sowie in die wissenschaftliche Literatur eingeordnet. Abschließend wird in Unterkapitel 1.3 die Struktur der Dissertationsschrift und das Forschungsdesign der drei wissenschaftlichen Studien erläutert.

Kapitel 2 umfasst die erste eigenständige Studie mit dem Titel ‚Cyberrisiken – Vom Begriffswirrwarr zu einem einheitlichen Begriffsverständnis'. Hinsichtlich der interdisziplinären Barrieren des Forschungsfelds und des Mangels an holistischen Ansätzen (Falco et al., 2019b) besteht das Ziel dieser Untersuchung in der systematischen und strukturierten inhaltlichen Auswertung

der in der theorie- und praxisnahen Literatur bekannten Definitionen des Terminus ‚Cyberrisiko' sowie in der Ableitung eines disziplinübergreifenden Begriffsmodells. Basierend auf der initialen Literaturrecherche (Randolph, 2009) werden mehr als 140 relevante Textpassagen und Äußerungen von 26 Definitionsansätzen des Begriffs ‚Cyberrisiko' auf inhaltliche Kriterien untersucht (Mayring, 2015). Durch Kodierung und Paraphrasierung des extrahierten Materials werden relevante und allgemeingültige Eigenschaften von Cyberrisiken abgeleitet und es wird eine neue umfassende Definition innerhalb eines Begriffsmodells postuliert. Das Cyberrisiko-Begriffsmodell kann sowohl als disziplinübergreifende Klammer um die bisherigen Definitionsansätze verstanden werden als auch zur Standardisierung und Vereinfachung der künftigen Cyberforschung beitragen. Zudem profitieren Unternehmen und Wirtschaft von einer einheitlichen Cyberrisiko-Terminologie, beispielsweise bei der Implementierung von ‚Cybermodulen' im Rahmen des Informationssicherheitsmanagementsystems (ISMS). Die erste Studie wurde bei der Zeitschrift *HMD – Praxis der Wirtschaftsinformatik* am 15.6.2022 angenommen und am 6.7.2022 online publiziert.

Kapitel 3 beinhaltet die zweite Studie mit dem Titel ‚Modelling and predicting enterprise-level cyber risks in the context of sparse data availability'. Aufgrund des Mangels an historischen Cybervorfällen (Eling & Schnell, 2016; Marotta et al., 2017; Boyer, 2020) und der im Umkehrschluss beschränkten Möglichkeiten eines quantitativen Cyberrisikomanagements (Palsson et al., 2020) schlägt dieses Forschungsvorhaben einen neuartigen quantitativen Bewertungsansatz vor, um Cyberrisiken auf Unternehmensebene zu bewerten. Die Analyse beruht auf der Öffentliche Schadenfälle OpRisk (ÖffSchOR)-Datenbank – einer Datenbank für operationelle Risiken (OpRisk), die sich auf öffentlich bekannt gegebene Schadenfälle im europäischen Finanzsektor fokussiert und bisher nicht in der Cyberrisiko-Forschung angewandt wurde. Aufbauend auf den Arbeiten von Shi & Yang (2018), Eling & Wirfs (2019) sowie Fang et al. (2021), werden die Eintrittswahrscheinlichkeit und das Ausmaß eines potenziellen Cybervorfalls vorhergesagt. Konkret wird die statistische Abhängigkeit basierend auf einer (D-Vine-)Copula-Struktur modelliert, um mit der Spärlichkeit der multivariaten Zeitreihe umgehen zu können. Dieser Ansatz schafft erste empirisch fundierte und quantitativ messbare Erkenntnisse über die tatsächlichen Cyberschäden auf Unternehmensebene. Dabei zeigt die Studie, dass einerseits Cyberrisiken im Mittel weniger schwerwiegend sind als in jüngsten Studien behauptet. Andererseits folgen Subindustrien unterschiedlichen Verteilungen und müssen separat modelliert werden. Ferner bestätigt sich die Erkenntnis, dass Cyberrisiken „heavy-tailed" sind (Foss et al., 2013) und ein Cybervorfall ein Unternehmen finanziell langfristig schädigen kann (Eling & Wirfs, 2019; Wheatley et al., 2021). Die skizzierte Methodik ermöglicht es Forschern, Praktikern sowie Cyberversicherern, das Cyberrisiko trotz des Mangels an größeren Datensätzen quantitativ zu bewerten und mit bestehenden Instrumenten der Preisgestaltung zu kombinieren, um risikobasierte Prämien zu berechnen (Nurse et al., 2020; Cremer

et al., 2022). Dieses Forschungsvorhaben ergänzt somit die begrenzten wissenschaftlichen Erkenntnisse über die empirische Quantifizierung von Cyberrisiken und trägt zu einem besseren Verständnis in diesem Bereich bei. Die zweite Studie wurde bei der Zeitschrift *The Geneva Papers on Risk and Insurance – Issues and Practice* am 1.12.2022 angenommen und am 10.12.2022 online publiziert.

Kapitel 4 fokussiert auf die dritte Studie mit dem Titel ‚Zur Cybersicherheit von Krankenhäusern – Eine empirische Bestandsaufnahme'. Zwar haben das Gesundheitswesen und die Patientenversorgung im Speziellen von der Digitalisierung profitiert, jedoch stellen Cyberrisiken das Krankenhausumfeld vor neue Herausforderungen (Argaw et al., 2020; Hoppe et al., 2021). Zudem finden sich bis dato nur beschränkte wissenschaftliche Erkenntnisse über den Umgang und das Management der Cybersicherheit im Gesundheitswesen, insbesondere aus dem europäischen und deutschsprachigen Raum (Sardi et al., 2020). Daher setzt sich der dritte Forschungsbeitrag zum Ziel, relevante Aspekte der Cybersicherheit von deutschen Krankenhäusern sowie Herausforderungen im Umgang mit Cyberrisiken zu erarbeiten. Aufgrund des neuartigen Forschungsfelds ist die Studie qualitativ-empirisch ausgelegt. Konkret werden 19 Experten aus dem Krankenhaus- und Gesundheitswesen befragt, um die Bedeutung und Implikationen zur Sicherstellung der Cybersicherheit im deutschen Gesundheitswesen zu bewerten. Gemäß der inhaltlich strukturierenden qualitativen Inhaltsanalyse nach Kuckartz & Rädiker (2022) werden neue Erkenntnisse generiert sowie Theorien und Hypothesen abgeleitet (Diekmann, 2007; Finfgeld-Connett, 2014; Schnell et al., 2018; Wrede et al., 2018). Die Ergebnisse verdeutlichen, dass Cyberrisiken als reale Bedrohung im Krankenhausumfeld wahrgenommen werden. Gleichwohl mangelt es an einer ausgeprägten Cyber Security Awareness sowie einer systematischen Implementierung und Integration des Cyberrisikomanagements. Zur Schaffung der erforderlichen Grundlagen und Strukturen bedarf es einer kontinuierlichen Finanzierung von Cybersicherheitsmaßnahmen, insbesondere vor dem Hintergrund der jahrzehntelangen Unterfinanzierung von Krankenhäusern (Schmitz & Pedell, 2013). Dieser Forschungsbeitrag schafft eine empirisch fundierte Diskussionsgrundlage für Krankenhäuser, das Gesundheitswesen und die Politik über den aktuellen Status quo und die zugrunde liegenden Herausforderungen zur langfristigen Sicherstellung der Cybersicherheit in diesem bedeutenden Segment der kritischen Infrastrukturen. Die dritte Studie wurde bei der Zeitschrift *Die Unternehmung – Swiss Journal of Business Research and Practice* angenommen.

In Kapitel 5 werden die Kernergebnisse zusammengefasst. Darüber hinaus werden deren Implikationen für Wissenschaft und Praxis erläutert, bevor die Dissertation mit einem Ausblick abgeschlossen wird.

1. Synopse

- Motivation und Hintergrund (1.1)
- Forschungsfragen und literarische Einbettung (1.2)
- Forschungsdesign und Struktur der Dissertation (1.3)

2. Studie 1: Cyberrisiken – Vom Begriffswirrwarr zu einem einheitlichen Begriffsverständnis

- Wie ist der Terminus ‚Cyberrisiko' in der wissenschaftlichen Literatur definiert?
- Inwiefern lässt sich der Terminus ‚Cyberrisiko' von verwandten Begrifflichkeiten formal abgrenzen?

3. Studie 2: Modelling and predicting enterprise-level cyber risks in the context of sparse data availability

- Wie und in welchem Umfang können Cyberereignisse modelliert und vorhergesagt werden?
- Inwiefern existieren Unterschiede hinsichtlich der Eintrittswahrscheinlichkeit und des Ausmaßes von Cyberereignissen über (Sub-)Industrien hinweg?

4. Studie 3: Zur Cybersicherheit von Krankenhäusern – Eine empirische Bestandsaufnahme

- Wie gestaltet sich die Cybersicherheit in deutschen Krankenhäusern?
- Welche Herausforderungen und Implikationen ergeben sich in der Zukunft zur Sicherstellung der Cybersicherheit im Gesundheitswesen?

5. Zusammenfassung

- Kernergebnisse und Implikationen für Wissenschaft und Praxis (5.1)
- Ausblick (5.2)

Abbildung 1-4: Struktur der Dissertationsschrift

	Studie 1	**Studie 2**	**Studie 3**
Titel	Cyberrisiken – Vom Begriffswirrwarr zu einem einheitlichen Begriffsverständnis	Modelling and predicting enterprise-level cyber risks in the context of sparse data availability	Zur Cybersicherheit von Krankenhäusern – Eine empirische Bestandsaufnahme
Methodologie	Qualitativ (Literaturrecherche, strukturierte Inhaltsanalyse, Ableitung eines Begriffsmodells)	Quantitativ (Zeitreihenanalyse, Logit-Regression, statistische Modellierung, Copula-Modelle, Extremwerttheorie)	Qualitativ (Experteninterviews, inhaltlich strukturierende Inhaltsanalyse)
Daten	Sekundärdaten: Wissenschaftliche Definitionen des Terminus Cyberrisiko	Sekundärdaten: Historische Cyberereignisse der ÖffSchOR-Datenbank	Primärdaten: Befragung von IT- und Cybersicherheitsexperten
Kontribution	Proposition eines umfassenden Begriffsmodells (Definition des Terminus ‚Cyberrisiko' und Abgrenzung zu verwandten Begrifflichkeiten)	Vorhersage der Eintrittswahrscheinlichkeit und des Ausmaßes eines Cyberereignisses für verschiedene Finanzinstitute	Erste wissenschaftliche Erkenntnisse über den Status quo und aktuelle Herausforderungen der Cybersicherheit im deutschen Gesundheitswesen
Status	Beitrag publiziert: Zängerle, D. & Schiereck, D. (2023). Cyberrisiken – Vom Begriffswirrwarr zu einem einheitlichen Begriffsverständnis. *HMD Praxis der Wirtschaftsinformatik*, *60*(1), 214–229. https://doi.org/10.1365/s40702-022-00888-3	Beitrag publiziert: Zängerle, D. & Schiereck, D. (2023). Modelling and predicting enterprise-level cyber risks in the context of sparse data availability. *The Geneva Papers on Risk and Insurance – Issues and Practice. 48*, 434–462. https://doi.org/10.1057/s41288-022-00282-6	Beitrag publiziert: Zängerle, D., & Schiereck, D. (2023). Zur Cybersicherheit von Krankenhäusern– Eine empirische Bestandsaufnahme. *Die Unternehmung*, *77*(4), 420–454. https://doi.org/10.5771/0042-059X-2023-4-420

Tabelle 1-2: Überblick des Forschungsvorhabens

2 Studie 1: Cyberrisiken – Vom Begriffswirrwarr zu einem einheitlichen Begriffsverständnis

von Daniel Zängerle und Dirk Schiereck

Zusammenfassung

Vor dem Hintergrund einer hochdynamischen Entwicklung weltweiter Cybervorfälle und der stetig wachsenden Bedeutung der Cyberforschung untersucht dieser Beitrag anhand einer systematischen und strukturierten Inhaltsanalyse die in der Wissenschaft und praxisnahen Literatur postulierten Definitionsansätze des Terminus Cyberrisiko und leitet ein disziplinübergreifendes Begriffsmodell als Basis für die künftige Cyberforschung und das operationelle Risikomanagement ab. Die Ergebnisse zeigen, dass es bislang keine einheitliche Begriffsdefinition für das Cyberrisiko gibt und die analysierten Definitionsansätze eine Vielzahl an unterschiedlichen Kernmerkmalen des Cyberrisikos zusammenfassen. Besonders häufig werden direkte und indirekte Auswirkungen, physische und digitale Risikoobjekte sowie beabsichtigte und sonstige Bedrohungen in den untersuchten Definitionen identifiziert, obgleich unbeabsichtigte Bedrohungen, insbesondere durch den Faktor Mensch als Einfallstor, nicht zu vernachlässigen sind. Das auf der Inhaltsanalyse basierende Begriffsmodell stellt eine umfassende Alternative zu den bisherigen, eher disziplinspezifischen Definitionsansätzen dar und trägt als elementarer Baustein in der Erarbeitung und dem aktuellen Diskurs über eine einheitliche Cyberterminologie bei.

Dieser Beitrag ist erschienen als:

Zängerle, D. & Schiereck, D. (2023). Cyberrisiken – Vom Begriffswirrwarr zu einem einheitlichen Begriffsverständnis. *HMD Praxis der Wirtschaftsinformatik*, *60*(1), 214–229. https://doi.org/10.1365/s40702-022-00888-3

3 Studie 2: Modelling and predicting enterprise-level cyber risks in the context of sparse data availability

von Daniel Zängerle und Dirk Schiereck

Abstract

Despite growing attention to cyber risks in research and practice, quantitative cyber risk assessments remain limited, mainly due to a lack of reliable data. This analysis leverages sparse historical data to quantify the financial impact of cyber incidents at the enterprise level. For this purpose, an operational risk database – which has not been previously used in cyber research – was examined to model and predict the likelihood, severity and time dependence of a company's cyber risk exposure. The proposed model can predict a negative time correlation, indicating that individual cyber exposure is increasing if no cyber loss has been reported in previous years, and vice versa. The results suggest that the probability of a cyber incident correlates with the subindustry, with the insurance sector being particularly exposed. The predicted financial losses from a cyber incident are less extreme than cited in recent investigations. The study confirms that cyber risks are heavy-tailed, jeopardising business operations and profitability.

Dieser Beitrag ist erschienen als:

Zängerle, D. & Schiereck, D. (2023). Modelling and predicting enterprise-level cyber risks in the context of sparse data availability. *The Geneva Papers on Risk and Insurance – Issues and Practice*. *48*, 434–462. https://doi.org/10.1057/s41288-022-00282-6

4 Studie 3: Zur Cybersicherheit von Krankenhäusern – Eine empirische Bestandsaufnahme

von Daniel Zängerle und Dirk Schiereck

Zusammenfassung

In Anbetracht der stetig steigenden Bedrohungslage durch Cyberrisiken untersucht dieser Beitrag Implikationen für das Cyberrisikomanagement in deutschen Krankenhäusern. Aufgrund des Facettenreichtums dieser Herausforderungen und der bislang noch unzureichenden Berücksichtigung in der wissenschaftlichen Forschung werden explorative Interviews mit Experten aus deutschen Krankenhäusern sowie des Gesundheitswesens geführt. Die Ergebnisse dieser Interviews verdeutlichen, dass Cyberrisiken als reale Bedrohung für Krankenhäuser wahrgenommen werden. Allerdings mangelt es noch an einer ausgeprägten Cyber Security Awareness sowie einer systematischen Implementierung und Integration des Cyberrisikomanagements.

Dieser Beitrag ist erschienen als:

Zängerle, D., & Schiereck, D. (2023). Zur Cybersicherheit von Krankenhäusern–Eine empirische Bestandsaufnahme. *Die Unternehmung, 77*(4), 420–454. https://doi.org/10.5771/0042-059X-2023-4-420

5 Zusammenfassung

Das übergeordnete Ziel dieser Dissertation ist es, das Verständnis über das Phänomen von Cyberrisiken in Wissenschaft und Praxis zu verbessern. Dazu wurden in dieser Abhandlung drei Forschungsbeiträge präsentiert, die das Cyberrisiko aus unterschiedlichen wirtschafts- und versicherungswissenschaftlichen Blickwinkeln beleuchten, die in Einklang mit der Forschungsagenda von Falco et al. (2019a) stehen. Zunächst wird in Kapitel 1 erläutert, dass sich einerseits die Bedrohungslage durch Cyberrisiken weiter zuspitzt und es andererseits am Bewusstsein für Cyberrisiken in Wissenschaft und Praxis mangelt. Aufgrund der Unklarheit über die Natur des Cyberrisikos und dessen Begrifflichkeit leitet der erste Forschungsbeitrag (Kapitel 2) ein theoriegeleitetes Begriffsmodell aus der Cyberrisiko-Literatur ab, das eine umfassende Definition des Terminus ‚Cyberrisiko' sowie eine konkrete Abgrenzung zu verwandten Begrifflichkeiten vorschlägt. Anschließend liefert der zweite Forschungsbeitrag (Kapitel 3) relevante Einblicke in die Quantifizierung und Bewertung von Cyberrisiken auf Unternehmensebene. Trotz des Mangels an großen Datenbanken schafft diese Studie erste empirische Erkenntnisse über die tatsächlichen Cyberrisikoschäden auf Unternehmensebene. Die dritte Studie (Kapitel 4) befasst sich mit dem Cyberrisikomanagement des deutschen Gesundheitswesens. In Hinblick auf die hohe Exponierung der kritischen Infrastruktur gegenüber Cyberbedrohungen gibt dieser Beitrag Aufschluss über den aktuellen Umgang und die Herausforderungen der Cybersicherheit deutscher Krankenhäuser.

5.1 Kernergebnisse und Implikationen für Wissenschaft und Praxis

Zusammenfassend und zur Beantwortung der in Unterkapitel 1.2 formulierten Forschungsfragen zeigt diese Dissertation, dass ...

- … sich aufgrund der Vielzahl unterschiedlicher Begriffsdefinitionen über die vergangenen Jahre der Terminus ‚Cyberrisiko' zu Verwirrung geführt hat und die Notwendigkeit einer einheitlichen Cyberterminologie besteht. (1a)
- … die begriffliche Abgrenzung zu verwandten Termini wie dem IT- oder IS-Risiko weder in der Forschung noch in der Praxis eindeutig existiert und sich insbesondere Überschneidungen ergeben, die die Verwirrungen hinsichtlich der Begrifflichkeit befeuern. (1b)
- … Cyberrisiken sich von operationellen Risiken unterscheiden und im Vergleich zu Nicht-Cyberrisiken im Durchschnitt niedriger, weniger schief und weniger extrem sind. Gleichwohl sind Cyberrisiken ‚heavy-tailed' und das individuelle Cyberrisiko steigt, sofern in den Vorjahren kein Cybervorfall gemeldet wurde. (2a)

- … Industrien und Subindustrien separat modelliert werden sollten. Konkret konnten unterschiedliche Eintrittswahrscheinlichkeiten und Schadensauswirkungen für Banken, Kommunalbanken, Versicherungen und weitere Finanzdienstleister nachgewiesen werden. (2b)
- … Cyberrisiken als reale Bedrohung für Krankenhäuser wahrgenommen werden, es allerdings an einer ausgeprägten Cyber Security Awareness sowie einer systematischen Implementierung und Integration des Cyberrisikomanagements mangelt. (3a)
- … die Krankenhäuser mit einer Vielzahl interner und externer Herausforderungen konfrontiert sind, die nur in einer gemeinschaftlichen Kraftanstrengung von Politik, Krankenkassen, Ländern, Interessenvertretungen und Privatwirtschaft gemeistert werden können. (3b)

Diese Dissertation leistet in mehrfacher Hinsicht einen Beitrag für Wissenschaft und Praxis. Das im ersten Beitrag (Kapitel 2) vorgeschlagene Begriffsmodell kann als Grundlage für ein einheitliches Begriffsverständnis für die weitere Cyberrisikoforschung fungieren. Zudem kann es die mangelnde Cyber Security Awareness in der Praxis verbessern, indem der Definitionsvorschlag des Terminus ‚Cyberrisiko' in einem unternehmensweiten Glossar aufgenommen und von verwandten Begrifflichkeiten eindeutig abgegrenzt wird. Im Vergleich zu den vorwiegend qualitativen Bewertungsansätzen von Cyberrisiken bietet der zweite Forschungsbeitrag (Kapitel 3) ein empirisch fundiertes Vorgehen zur quantitativen Bewertung von Cyberrisiken auf Unternehmensebene. Darüber hinaus helfen die Ergebnisse Risikomanagern, Versicherern und politischen Entscheidungsträgern, ein quantitatives und datengestütztes Cyberrisikomanagement zu entwickeln. Insbesondere steht die Versicherungsbranche vor großen Herausforderungen bei der Bewertung von Cyberrisiken, sodass das vorgeschlagene Modell in bestehende Preisgestaltungsinstrumente und Faktoren von Cyberversicherungen integriert werden kann, um Cyberpolicen und risikobasierte Prämien besser zu bewerten. Aufgrund des Mangels an bestehenden Forschungsarbeiten über das Management der Cybersicherheit im Gesundheitswesen schafft die dritte Studie (Kapitel 4) ein erstes, umfassendes Verständnis über den aktuellen Status quo und die zugrunde liegenden Herausforderungen und Auswirkungen. Auf Basis dieser Ergebnisse bieten sich weitere wissenschaftliche Untersuchungen an, die die identifizierten Themenbereiche näher beleuchten. Für die Praxis bietet das dritte Forschungspapier die erforderliche Diskussionsgrundlage zwischen Krankenhäusern, der Gesundheitsbranche und politischen Entscheidungsträgern, wie die Cybersicherheit in diesem bedeutenden Segment der kritischen Infrastruktur langfristig gewährleistet werden kann.

Trotz der Vielzahl relevanter Ergebnisse und Implikationen für Wissenschaft und Praxis unterliegt diese Dissertation bestimmten Limitationen, die vielversprechende Ansätze für die

zukünftige Forschung bieten können. Aufgrund der qualitativ ausgerichteten Vorgehensweise der ersten Studie (Kapitel 2) kann die Vollständigkeit der in der Literatur vorliegenden Cyberdefinitionen abschließend nicht garantiert werden, weshalb die Verallgemeinerbarkeit der gewonnenen Erkenntnisse eingeschränkt sein kann. Ferner beruhen die Kategorisierung und die Auswertung der Begriffsvorschläge auf der subjektiven Wahrnehmung der Autoren, was Verzerrungen der Erkenntnisse bedingen kann. Der zweite Forschungsbeitrag (Kapitel 3) unterliegt insbesondere methodologischen und datenbezogenen Restriktionen. Zum einen kann die Verwendung historischer Daten zur Vorhersage zukünftiger Cyberereignisse in der schnelllebigen Welt hinterfragt werden, zumal die ÖffSchOR-Datenbank ihre Informationen aus Print- und Online-Medien bezieht und somit nur einen Teil der tatsächlich verfügbaren Cyberereignisse abdeckt. Zum anderen können die Modellierungsannahmen, beispielsweise die Unabhängigkeit der betrachteten Unternehmen sowie die Modellierung einer einzelnen Schadenskategorie, die quantitativen Ergebnisse verzerren. Abschließend können Repräsentativität und Objektivität der Forschungsergebnisse der dritten Studie (Kapitel 4) infrage gestellt werden. Die Analyse beruht auf mündlichen Erfahrungen einzelner IT- und Cybersicherheitsexperten deutscher Krankenhäuser. Ferner kann die Verallgemeinerung der Ergebnisse aufgrund der zielgerichteten Stichprobe und der relativ kleinen Stichprobengröße eingeschränkt sein.

5.2 Ausblick

Diese Arbeit zeigt, dass Cyberrisiken eine aktuelle und bedeutende Herausforderung für Unternehmen, Politik und Versicherer darstellen. Die drei Forschungsbeiträge bieten relevante wirtschafts- und versicherungswissenschaftliche Erkenntnisse zur Beantwortung elementarer Grundsatzfragen sowie zur Schaffung eines besseren Verständnisses über die Natur des Cyberrisikos (Falco et al., 2019a; Eling, 2020). Cyberrisiken können in vielen Bereichen der heutigen digitalisierten Welt auftreten und bedrohen nicht nur Verbraucher und Unternehmen, sondern gleichsam die kritische Infrastruktur und schlussendlich das Wohl der Gesellschaft (Njegomir & Marović, 2012; Choudhry, 2014; Bendovschi, 2015; Wrede et al., 2018; Aldasoro et al., 2020). Hinsichtlich der weiter voranschreitenden Digitalisierung und Vernetzung der IT verschärft sich die Gefahrenlage durch Cyberrisiken weiter (Rakes et al., 2012; Aldasoro et al., 2020), weshalb diese Arbeit nur als erster Schritt in Richtung eines umfassenden Verständnisses über das Phänomen Cyberrisiken betrachtet werden kann. Daher ist eine tiefere Integration verschiedener Sichtweisen und Disziplinen für die weitere Cyberrisiko-Forschung von elementarer Bedeutung (Falco et al., 2019b; Strupczewski, 2021). Insbesondere bedarf es einer einheitlichen Cyberterminologie, die es in Zusammenarbeit mit unterschiedlichen Interessenvertretungen, Industrien, Ländern und (inter-)nationalen Organisationen zu erarbeiten gilt. Mit besseren und umfangreicheren

Datenbanken können genauere quantitative Modelle entwickelt werden, die weitere Dimension und Sichtweisen berücksichtigen (Fahrenwaldt et al., 2018; Jevtić & Lanchier, 2020; Palsson et al., 2020; Wu et al., 2021). Ferner ergeben sich an der Schnittstelle resilienter Organisationen der kritischen Infrastruktur und der langfristigen Sicherstellung der Cybersicherheit weitere relevante Forschungsfragen.

Durch die charakterisierte Komplexität und Dynamik des Cyberrisikos entwickelt sich ein relevantes Forschungsfeld, das in Zeiten von Internet der Dinge, Kryptowährungen und Künstlicher Intelligenz immer mehr an Bedeutung gewinnen wird (Zängerle & Schiereck, 2023a).

6 Literaturverzeichnis

Aas, K., Czado, C., Frigessi, A. & Bakken, H. (2009). Pair-copula constructions of multiple dependence. *Insurance: Mathematics and Economics*, *44*(2), 182–198. https://doi.org/10.1016/j.insmatheco.2007.02.001

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, *33*(3), 237–248. https://doi.org/10.1080/0144929X.2012.708787

Abraham, C., Chatterjee, D. & Sims, R. R. (2019). Muddling through cybersecurity: Insights from the U.S. healthcare industry. *Business Horizons*, *62*(4), 539–548. https://doi.org/10.1016/j.bushor.2019.03.010

Acar, E. F., Czado, C. & Lysy, M. (2019). Flexible dynamic vine copula models for multivariate time series data. *Econometrics and Statistics*, *12*, 181–197. https://doi.org/10.1016/j.ecosta.2019.03.002

AG Hochschulmedizin (2014). Neue Finanzierung der Universitätsklinika dringend notwendig. *Orthopädie und Unfallchirurgie - Mitteilungen und Nachrichten*, *03*(01), 13–14. https://doi.org/10.1055/s-0034-1368736

Alberts, C. J., Behrens, S. G., Pethia, R. D. & Wilson, W. R. (1999). *Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework, Version 1.0.* https://doi.org/10.21236/ada367718

Aldasoro, I., Gambacorta, L., Giudici, P. & Leach, T. (2020). *The drivers of cyber risk.* BIS Working Papers No 865. Bank for International Settlements. https://www.bis.org/publ/work865.pdf. Zugegriffen: 20.05.2021

Ale, B., Burnap, P. & Slater, D. (2015). On the origin of PCDS – Probability consequence diagrams. *Safety Science*, *72*, 229–239. https://doi.org/10.1016/j.ssci.2014.09.003

Almulhem, A. (2012). Threat modeling for electronic health record systems. *Journal of Medical Systems*, *36*(5), 2921–2926. https://doi.org/10.1007/s10916-011-9770-6

Anderson, S. & Williams, T. (2018). Cybersecurity and medical devices: Are the ISO/IEC 80001-2-2 technical controls up to the challenge? *Computer Standards & Interfaces*, *56*(C), 134–143. https://doi.org/10.1016/j.csi.2017.10.001

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M.-V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.-M., O'Leary, C., Eshaya-Chauvin, B. & Flahault, A. (2020). Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making*, *20*(1), 146. https://doi.org/10.1186/s12911-020-01161-7

Ashby, S., Buck, T., Nöth-Zahn, S. & Peisl, T. (2018). Emerging IT Risks: Insights from German Banking. *The Geneva Papers on Risk and Insurance - Issues and Practice*, *43*(2), 180–207. https://doi.org/10.1057/s41288-018-0081-8

Augurzky, B., Bschor, T., Busse, R., Dötsch, J., Evans, M., Felix, D., Gürkan, I., Haeske-Seeberg, H., Hasseler, M., Huster, S., Karagiannidis, C., Kingreen, T., Kroemer, H., Münkler, L., Schmitt, J., Somasundaram, R. & Sundmacher, L. (2022). *Grundlegende Reform der Krankenhausvergütung: Dritte Stellungnahme und Empfehlung der Regierungskommission für eine moderne und bedarfsgerechte Krankenhausversorgung*. http://www.bundesgesundheitsministerium.de/krankenhauskommission-stellungnahme-krankenhausverguetung.pdf. Zugegriffen: 03.01.2023

Bandyopadhyay, T., Mookerjee, V. S. & Rao, R. C. (2009). Why IT managers don't go for cyber-insurance products. *Communications of the ACM*, *52*(11), 68–73. https://doi.org/10.1145/1592761.1592780

Baur, N. & Blasius, J. (Hrsg.). (2014). *Handbuch Methoden der empirischen Sozialforschung*. Springer VS.

Bedford, T. & Cooke, R. M. (2002). Vines: A New Graphical Model for Dependent Random Variables. *The Annals of Statistics*, *30*(4), 1031–1068. http://www.jstor.org/stable/1558694.

Bendovschi, A. (2015). Cyber-attacks – Trends, patterns and security countermeasures. *Procedia Economics and Finance*, *28*, 24–31. https://doi.org/10.1016/S2212-5671(15)01077-1

Berger, S., Bürger, O. & Röglinger, M. (2020). Attacks on the Industrial Internet of Things – Development of a multi-layer Taxonomy. *Computers & Security*, *93*, 101790. https://doi.org/10.1016/j.cose.2020.101790

Biener, C., Eling, M. & Wirfs, J. (2015). Insurability of Cyber Risk: An Empirical Analysis. *The Geneva Papers on Risk and Insurance - Issues and Practice*, *40*(1), 131–158. https://doi.org/10.1057/gpp.2014.19

Bank for International Settlements (BIS). (2016). *Guidance on cyber resilience for financial market infrastructures*. https://www.bis.org/cpmi/publ/d146.pdf. Zugegriffen: 06.04.2021

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Bitkom). (2019). *Wirtschaftsschutz in der digitalen Wirtschaft*. https://www.bitkom.org/sites/default/files/2019-11/bitkom_wirtschaftsschutz_2019_0.pdf. Zugegriffen: 20.04.2021

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Bitkom). (2022). *Wirtschaftsschutz 2022*. https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022#_. Zugegriffen: 15.01.2023

Bitzer, M., Stahl, B. & Strobel, J. (2021). Empathy for Hackers – An IT Security Risk Assessment Artifact for Targeted Hacker Attacks. *ECIS 2021 Research Papers*(41). https://aisel.aisnet.org/ecis2021rp/41. Zugegriffen: 04.10.2022

Bundeskriminalamt (BKA). (2021). *Cybercrime: Bundeslagebild 2020*. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2020.html?nn=28110. Zugegriffen: 11.05.2021

Blanke, S. J. & McGrady, E. (2016). When it comes to securing patient health information from breaches, your best medicine is a dose of prevention: A cybersecurity risk assessment checklist. *Journal of Healthcare Risk Management*, *36*(1), 14–24. https://doi.org/10.1002/jhrm.21230

Böhme, R. & Kataria, G. (2006). *Models and measures for correlation in cyber-insurance*. Workshop on the Economics of Information Security (WEIS). https://core.ac.uk/download/pdf/162458449.pdf. Zugegriffen: 11.02.2021

Böhme, R., Laube, S. & Riek, M. (2019). A fundamental approach to cyber risk analysis. *Casualty Actuarial Society*, *12*(2), 161–185. https://www.variancejournal.org/issues/12-02/161.pdf. Zugegriffen: 08.02.2021

Boudko, S. & Abie, H. (2019). Adaptive Cybersecurity Framework for Healthcare Internet of Things. In *2019 13th International Symposium on Medical Information and Communication Technology (ISMICT),* Oslo, Norway.

Bouveret, A. (2018). *Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment*. IMF Working Papers. https://doi.org/10.5089/9781484360750.001

Boyer, M. M. (2020). Cyber insurance demand, supply, contracts and cases. *The Geneva Papers on Risk and Insurance - Issues and Practice*, *45*(4), 559–563. https://doi.org/10.1057/s41288-020-00188-1

Bundesamt für Sicherheit in der Informationstechnik (BSI). (2021). *Glossar der Cyber-Sicherheit*. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Glossar-der-Cyber-Sicherheit/Functions/glossar.html;jsessionid=326A2F2D3A41CC886D6B4B2B4F7D21A4.internet082?nn=522504&cms_lv2=132798. Zugegriffen: 07.04.2021

Bundesamt für Sicherheit in der Informationstechnik (BSI). (2022). *Die Lage der IT-Sicherheit in Deutschland 2022*. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.html?nn=129410. Zugegriffen: 11.01.2023

Bulgurcu, Cavusoglu & Benbasat (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly*, *34*(3), 523. https://doi.org/10.2307/25750690

Bursig, H.-P. (2019). Cybersicherheit Vernetzter Medizinprodukte: Neue Herausforderungen. *kma - Klinik Management aktuell*, *24*(06), 76–77. https://doi.org/10.1055/s-0039-1692811

Camillo, M. (2017). Cyber risk and the changing role of insurance. *Journal of Cyber Policy*, *2*(1), 53–63. https://doi.org/10.1080/23738871.2017.1296878

Caruso, R. J. & Masters, M. (2014). Applying cyber risk management to medical device design. *Biomedical instrumentation & technology*, 32–37. https://doi.org/10.2345/0899-8205-48.s1.32

Cavusoglu, H., Mishra, B. & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, *9*(1), 69–104. https://doi.org/10.1080/10864415.2004.11044320

Cebula, J. J. & Young, L. R. (2010). *A taxonomy of operational cyber security risks*. Technical Note CMU/SEI-2010-TN-028. Software Engineering Institute. https://apps.dtic.mil/sti/pdfs/ADA537111.pdf. Zugegriffen: 10.02.2021

Cepeda, G. & Martin, D. (2005). A review of case studies publishing in Management Decision 2003-2004. *Management Decision*, *43*(6), 851–876. https://doi.org/10.1108/00251740510603600

Chavez-Demoulin, V., Embrechts, P. & Hofert, M. (2016). An Extreme Value Approach for Modeling Operational Risk Losses Depending on Covariates. *Journal of Risk and Insurance*, *83*(3), 735–776. https://doi.org/10.1111/jori.12059

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

Clarke, R. & Youngstein, T. (2017). Cyberattack on Britain's National Health Service - A Wake-up Call for Modern Medicine. *The New England journal of medicine*, *377*(5), 409–411. https://doi.org/10.1056/NEJMp1706754

Commission Nationale Pour La Protection Des Données (CNPD). (2022). *Decision regarding Amazon Europe Core S.à r.l.* https://cnpd.public.lu/en/actualites/international/2021/08/decision-amazon-2.html. Zugegriffen: 17.02.2022

Continental. (2023). *Cyberangriff auf Continental*. https://www.continental.com/de/presse/studien-publikationen/sonstige-publikationen/cyber-angriff-fragen-und-antworten/. Zugegriffen: 17.02.2023

Coronado, A. J. & Wong, T. L. (2014). Healthcare cybersecurity risk management: keys to an effective plan. *Biomedical Instrumentation & Technology*, *48*, 26–30. https://doi.org/10.2345/0899-8205-48.s1.26

Cox, L. A., Jr. (2012). Evaluating and Improving Risk Formulas for Allocating Limited Budgets to Expensive Risk-Reduction Opportunities. *Risk Analysis*, *32*(7), 1244–1252. https://doi.org/10.1111/j.1539-6924.2011.01735.x

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F. & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *The Geneva Papers on Risk and Insurance - Issues and Practice*, *47*(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6

CRO Forum. (2014). *Cyber resilience - the cyber risk challenge and the role of insurance*. https://www.thecroforum.org/wp-content/uploads/2015/01/Cyber-Risk-Paper-version-24-1.pdf. Zugegriffen: 01.04.2021

CRO Forum. (2016). *Concept paper on a proposed categorisation methodology for cyber risk*. https://www.thecroforum.org/2016/06/20/concept-proposal-categorisation-methodology-for-cyber-risk/. Zugegriffen: 06.04.2021

Darms, M., Haßfeld, S. & Fedtke, S. (2019). *IT-Sicherheit und Datenschutz im Gesundheitswesen*. Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-21589-7

Davey, J. (1995). The role of risk analysis in European harmonisation of security for healthcare information systems. *Computer Methods and Programs in Biomedicine*, *48*(1), 133–137. https://doi.org/10.1016/0169-2607(95)01673-H

Deane, J. K., Ragsdale, C. T., Rakes, T. R. & Rees, L. P. (2009). Managing supply chain risk and disruption from IT security incidents. *Operations Management Research*, *2*(1-4), 4–12. https://doi.org/10.1007/s12063-009-0018-2

Diekmann, A. (2007). *Empirische Sozialforschung: Grundlagen, Methoden, Anwendungen* (14. Aufl.). *rororo: Rowohlts Enzyklopädie*. Rowohlt Taschenbuch Verlag.

European Banking Authority (EBA). (2019). *Final report: EBA guidelines on ICT and security risk management*. https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management. Zugegriffen: 07.04.2021

Eckert, C., Gatzert, N. & Heidinger, D. (2020). Empirically assessing and modeling spillover effects from operational risk events in the insurance industry. *Insurance: Mathematics and Economics*, *93*, 72–83. https://doi.org/10.1016/j.insmatheco.2020.04.003

Edwards, B., Hofmeyr, S. & Forrest, S. (2016). Hype and heavy tails: A closer look at data breaches. *Journal of Cybersecurity*, *2*(1), 3–14. https://doi.org/10.1093/cybsec/tyw003

Eisenhardt, K. M. (1989). Building Theories from Case Study Research. *The Academy of Management Review*, *14*(4), 532. https://doi.org/10.2307/258557

Eling, M. (2018). Cyber Risk and Cyber Risk Insurance: Status Quo and Future Research. *The Geneva Papers on Risk and Insurance - Issues and Practice*, *43*(2), 175–179. https://doi.org/10.1057/s41288-018-0083-6

Eling, M. (2020). Cyber risk research in business and actuarial science. *European Actuarial Journal*, *10*(2), 303–333. https://doi.org/10.1007/s13385-020-00250-1

Eling, M. & Jung, K. (2018). Copula approaches for modeling cross-sectional dependence of data breach losses. *Insurance: Mathematics and Economics*, *82*, 167–180. https://doi.org/10.1016/j.insmatheco.2018.07.003

Eling, M. & Loperfido, N. (2017). Data breaches: Goodness of fit, pricing, and risk measurement. *Insurance: Mathematics and Economics*, *75*, 126–136. https://doi.org/10.1016/j.insmatheco.2017.05.008

Eling, M. & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? *The Journal of Risk Finance*, *17*(5), 474–491. https://doi.org/10.1108/JRF-09-2016-0122

Eling, M., Schnell, W. & Sommerrock, F. (2016). *Ten key questions on cyber risk and cyber risk insurance.* The Geneva Assocation. https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/cyber-risk-10_key_questions.pdf. Zugegriffen: 06.04.2021

Eling, M. & Wirfs, J. H. (2016a). *Cyber risk: Too big to insure? Risk transfer options for a mercurial risk class.* Verlag Institut für Versicherungswirtschaft der Universität St. Gallen. I.VW HSG SchriftenreiheUR. http://hdl.handle.net/10419/226644. Zugegriffen: 06.04.2021

Eling, M. & Wirfs, J. H. (2016b). *Modelling and management of cyber risk.* Working Paper. http://www.actuaries.org/oslo2015/papers/iaals-wirfs&eling.pdf. Zugegriffen: 05.04.2021

Eling, M. & Wirfs, J. (2019). What are the actual costs of cyber risk events? *European Journal of Operational Research*, *272*(3), 1109–1119. https://doi.org/10.1016/j.ejor.2018.07.021

Epstein, E. S. (1969). A Scoring System for Probability Forecasts of Ranked Categories. *Journal of Applied Meteorology (1962-1982)*, *8*(6), 985–987. http://www.jstor.org/stable/26174707.

Etges, A. P. B. d. S., Grenon, V., Lu, M., Cardoso, R. B., Souza, J. S. de, Kliemann Neto, F. J. & Felix, E. A. (2018). Development of an enterprise risk inventory for healthcare. *BMC Health Services Research*, *18*(1), Artikel 578, 1–16. https://doi.org/10.1186/s12913-018-3400-7

European Data Protection Board (EDPD). (2021). *Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR*. https://edpb.europa.eu/system/files/2021-09/edpb_bindingdecision_202101_ie_sa_whatsapp_redacted_en.pdf. Zugegriffen: 17.02.2022

European Union (2013). *Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and amending Regulation (EU) No 648/2012 (Text with EEA relevance)*. http://data.europa.eu/eli/reg/2013/575/2022-07-08. Zugegriffen: 21.09.2022

European Union (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679. Zugegriffen: 14.02.2022

Fahrenwaldt, M. A., Weber, S. & Weske, K. (2018). Pricing of cyber insurance contracts in a network model. *ASTIN Bulletin*, *48*(3), 1175–1218. https://doi.org/10.1017/asb.2018.23

Falco, G., Eling, M., Jablanski, D., Miller, V., Gordon, L. A., Wang, S., Schmit, J., Thomas, R., Elvedi, M., Maillart, T., Donavan, E., Dejung, S., Weber, M., Durand, E., Nutter, F., Scheffer, U., Arazi, G., Ohana, G. & Lin, H. (2019a). *A Research Agenda for Cyber Risk and Cyber Insurance* (Weis). https://weis2016.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_35.pdf. Zugegriffen: 08.02.2021

Falco, G., Eling, M., Jablanski, D., Weber, M., Miller, V., Gordon, L. A., Wang, S. S., Schmit, J., Thomas, R., Elvedi, M., Maillart, T., Donavan, E., Dejung, S., Durand, E., Nutter, F., Scheffer, U., Arazi, G., Ohana, G. & Lin, H. (2019b). Cyber risk research impeded by disciplinary barriers. *Science*, *366*(6469), 1066–1069. https://doi.org/10.1126/science.aaz4795

Fang, Z., Xu, M., Xu, S. & Hu, T. (2021). A Framework for Predicting Data Breach Risk: Leveraging Dependence to Cope With Sparsity. *IEEE Transactions on Information Forensics and Security*, *16*, 2186–2201. https://doi.org/10.1109/TIFS.2021.3051804

Fayans, I., Motro, Y., Rokach, L., Oren, Y. & Moran-Gilad, J. (2020). Cyber security threats in the microbial genomics era: implications for public health. *Eurosurveillance*, *25*(6), 1900574. https://doi.org/10.2807/1560-7917.ES.2020.25.6.1900574

Fernando, J. I. & Dawson, L. L. (2009). The health information system security threat lifecycle: an informatics theory. *International Journal of Medical Informatics*, *78*(12), 815–826. https://doi.org/10.1016/j.ijmedinf.2009.08.006

Finfgeld-Connett, D. (2014). Use of content analysis to conduct knowledge-building and theory-generating qualitative systematic reviews. *Qualitative Research*, *14*(3), 341–352. https://doi.org/10.1177/1468794113481790

Foss, S., Korshunov, D. & Zachary, S. (2013). *An Introduction to Heavy-Tailed and Subexponential Distributions*. Springer New York. https://doi.org/10.1007/978-1-4614-7101-1

Früh, W. (2017). *Inhaltsanalyse: Theorie und Praxis* (9. Aufl.). *utb-studi-e-book: Bd. 2501*. UVK Verlagsgesellschaft mbH.

Financial Stability Board (FSB). (2018). *Cyber lexicon*. https://www.fsb.org/wp-content/uploads/P121118-1.pdf. Zugegriffen: 06.04.2021

Fu, K. & Blum, J. (2013). Controlling for cybersecurity risks of medical device software. *Communications of the ACM*, *56*(10), 35–37. https://doi.org/10.1145/2508701

United States General Accounting Office (GAO). (1996). *Content analysis: A methodology for structuring and analyzing written material.* GAO/PEMD-10.3.1. https://www.gao.gov/assets/pemd-10.3.1.pdf. Zugegriffen: 18.05.2021

Gioia, D. A., Corley, K. G. & Hamilton, A. L. (2013). Seeking Qualitative Rigor in Inductive Research. *Organizational Research Methods*, *16*(1), 15–31. https://doi.org/10.1177/1094428112452151

Giudici, P. & Raffinetti, E. (2020). Cyber risk ordering with rank-based statistical models. *AStA Advances in Statistical Analysis.* https://doi.org/10.1007/s10182-020-00387-0

Gläser, J. & Laudel, G. (2012). *Experteninterviews und qualitative Inhaltsanalyse als Instrumente rekonstruierender Untersuchungen*. *Lehrbuch*. VS, Verl. für Sozialwiss.

Gneiting, T. & Raftery, A. E. (2007). Strictly Proper Scoring Rules, Prediction, and Estimation. *Journal of the American Statistical Association*, *102*(477), 359–378. https://doi.org/10.1198/016214506000001437

Gordon, L. A. & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security*, *12*(4), 105–125. https://doi.org/10.1007/1-4020-8090-5_9

Gordon, L. A., Loeb, M. P. & Sohail, T. (2003). A framework for using insurance for cyber-risk management. *Communications of the ACM*, *46*(3), 81–85. https://doi.org/10.1145/636772.636774

Guy Carpenter. (2013). *Tomorrow never knows: Emerging risks report*. https://www.curie.org/sites/default/files/Emerging-Risks-Report-Sept-2013.pdf. Zugegriffen: 07.04.2021

Haas, A. & Hofmann, A. (2014). Risiken aus der Nutzung von Cloud-Computing-Diensten: Fragen des Risikomanagements und Aspekte der Versicherbarkeit. *Zeitschrift für die gesamte Versicherungswissenschaft*, *103*(4), 377–407. https://doi.org/10.1007/s12297-014-0285-3

Handelsblatt. (2021). *Colonial zahlte wohl fünf Millionen Dollar Lösegeld an Hacker*. https://www.handelsblatt.com/unternehmen/energie/medienbericht-cyberangriff-auf-benzin-pipeline-colonial-zahlte-wohl-fuenf-millionen-dollar-loesegeld/27188044.html. Zugegriffen: 18.05.2021

Haufe, K., Dzombeta, S. & Brandis, K. (2014). Proposal for a Security Management in Cloud Computing for Health Care. *The Scientific World Journal*, *2014*, 146970. https://doi.org/10.1155/2014/146970

He, Y. & Johnson, C. (2015). Improving the redistribution of the security lessons in healthcare: An evaluation of the Generic Security Template. *International Journal of Medical*

Informatics, *84*(11), 941–949. https://doi.org/10.1016/j.ijmedinf.2015.08.010

Heitzenrater, C. D. & Simpson, A. C. (2016). Policy, statistics and questions: Reflections on UK cyber security disclosures. *Journal of Cybersecurity*, *2*(1), 43–56. https://doi.org/10.1093/cybsec/tyw008

Herath, H. S. B. & Herath, T. C. (2011). Copula-based actuarial model for pricing cyber-insurance policies. *Insurance Markets and Companies: Analyses and Actuarial Computations*, *2*(1). https://businessperspectives.org/images/pdf/applications/publishing/templates/article/assets/3934/imc_2011_1_herath.pdf. Zugegriffen: 29.02.2021

Hiller, J. S. & Russell, R. S. (2013). The challenge and imperative of private sector cybersecurity: An international comparison. *Computer Law & Security Review*, *29*(3), 236–245. https://doi.org/10.1016/j.clsr.2013.03.003

Holden, W. L. (2015). The vital role of device manufacturers as cybercitizens. *Biomedical Instrumentation & Technology*, *49*(6), 410–422. https://doi.org/10.2345/0899-8205-49.6.410

Hoppe, F., Gatzert, N. & Gruner, P. (2021). Cyber risk management in SMEs: insights from industry surveys. *The Journal of Risk Finance*, *22*(3/4), 240–260. https://doi.org/10.1108/JRF-02-2020-0024

Huang, L.-C., Chu, H.-C., Lien, C.-Y., Hsiao, C.-H. & Kao, T. (2009). Privacy preservation and information security protection for patients' portable electronic health records. *Computers in Biology and Medicine*, *39*(9), 743–750. https://doi.org/10.1016/j.compbiomed.2009.06.004

Hubbard, D. W. & Seiersen, R. (2016). *How to measure anything in cybersecurity risk*. Wiley.

IBM Security. (2020). *Cost of a Data Breach Report 2020*. https://www.ibm.com/security/data-breach. Zugegriffen: 25.05.2021

Innerhofer-Oberperfler, F. & Breu, R. (2010). Potential Rating Indicators for Cyberinsurance: An Exploratory Qualitative Study. In T. Moore, D. Pym & C. Ioannidis (Hrsg.), *Economics of Information Security and Privacy* (S. 249–278). Springer US. https://doi.org/10.1007/978-1-4419-6967-5_13

The Institute of Risk Management (IRM). (2014). *Cyber risk - Resources for practitioners*. https://www.theirm.org/media/7237/irm-cyber-risk-resources-for-practitioners.pdf. Zugegriffen: 06.04.2021

International Standard Organisation (ISO). (2018). *ISO/IEC 27000:2018: Information technology - Security techniques - Information security management systems - Overview and vocabulary*. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC). https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en. Zugegriffen: 20.04.2021

Iwaya, L. H., Fischer-Hübner, S., Åhlfeldt, R.-M. & Martucci, L. A. (2019). Mobile health systems for community-based primary care: Identifying controls and mitigating privacy threats. *JMIR mHealth and uHealth*, *7*(3), e11642. https://doi.org/10.2196/11642

Järveläinen, J. (2013). IT incidents and business impacts: Validating a framework for continuity management in information systems. *International Journal of Information Management*, *33*(3), 583–590. https://doi.org/10.1016/j.ijinfomgt.2013.03.001

Jevtić, P. & Lanchier, N. (2020). Dynamic structural percolation model of loss distribution for cyber risk of small and medium-sized enterprises for tree-based LAN topology. *Insurance: Mathematics and Economics*, *91*, 209–223. https://doi.org/10.1016/j.insmatheco.2020.02.005

Joe, H. (1997). *Multivariate Models and Multivariate Dependence Concepts*. Chapman and Hall/CRC. https://doi.org/10.1201/9780367803896

Joe, H. (2005). Asymptotic efficiency of the two-stage estimation method for copula-based models. *Journal of Multivariate Analysis*, *94*(2), 401–419. https://doi.org/10.1016/j.jmva.2004.06.003

Jump, M. (2019). AAMI TIR97: A vital resource in the postmarket management of medical device security. *Biomedical Instrumentation & Technology*, *53*(6), 462–464. https://doi.org/10.2345/0899-8205-53.6.462

Jung, K. (2019). *Probable maximum cyber loss: Empirical estimation and reinsurance design with private-public partnership.* 2019 German Insurance Science Association (DVfVW) annual meeting. Berlin.

Kaiser, R. (2014). *Qualitative Experteninterviews: Konzeptionelle Grundlagen und praktische Durchführung*. *Elemente der Politik*. Springer. https://doi.org/10.1007/978-3-658-02479-6

Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A. & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, *139*(3), 719–749. https://doi.org/10.1016/j.jfineco.2019.05.019

Kamoun, F. & Nicho, M. (2014). Human and organizational factors of healthcare data breaches: The Swiss cheese model of data breach Causation And Prevention. *International Journal of Healthcare Information Systems and Informatics*, *9*(1), 42–60. https://doi.org/10.4018/ijhisi.2014010103

Kaspereit, T., Lopatta, K., Pakhchanyan, S. & Prokop, J. (2017). Systemic operational risk: spillover effects of large operational losses in the European banking industry. *The Journal of Risk Finance*, *18*(3), 252–267. https://doi.org/10.1108/JRF-11-2016-0141

Kayworth, T. & Whitten, D. (2012). *Effective information security requires a balance of social and technology factors* (Nr. 3). MIS Quarterly Executive. https://ssrn.com/abstract=2058035. Zugegriffen: 19.05.2021

Kesan, J. P. & Zhang, L. (2019). Analysis of Cyber Incident Categories Based on Losses. *SSRN Electronic Journal.* https://doi.org/10.2139/ssrn.3489436

Kim, H.-W., Park, J. H. & Jeong, Y.-S. (2018). Human-intelligence workflow management for the big data of augmented reality on cloud infrastructure. *Neurocomputing*, *279*, 19–26. https://doi.org/10.1016/j.neucom.2017.04.082

Knoll, M. & Strahringer, S. (2017). IT-GRC-Management im Zeitalter der Digitalisierung. In M. Knoll & S. Strahringer (Hrsg.), *IT-GRC-Management – Governance, Risk und Compliance: Grundlagen und Anwendungen* (S. 1–24). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-20059-6_1

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

Kosub, T. (2015). Components and challenges of integrated cyber risk management. *Zeitschrift für die gesamte Versicherungswissenschaft*, *104*(5), 615–634. https://doi.org/10.1007/s12297-015-0316-8

Kritzinger, E. & Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. *Computers & Security*, *27*(5-6), 224–231. https://doi.org/10.1016/j.cose.2008.05.006

Kruger, H. A. & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security*, *25*(4), 289–296. https://doi.org/10.1016/j.cose.2006.02.008

Kruse, J. (2015). *Qualitative Interviewforschung: Ein integrativer Ansatz* (2. Aufl.). *Grundlagentexte Methoden*. Beltz Juventa.

Kucera, M. (2020). Uniklinik Düsseldorf: Cyberangriff verursacht Todesfall. *kma - Klinik Management aktuell*, *25*(10), 6. https://doi.org/10.1055/s-0040-1718794

Kuckartz, U. & Rädiker, S. (2020). *Fokussierte Interviewanalyse mit MAXQDA: Schritt für Schritt* (1. Aufl.). Springer Fachmedien Wiesbaden; Springer VS.

Kuckartz, U. & Rädiker, S. (2022). *Qualitative Inhaltsanalyse: Methoden, Praxis, Computerunterstützung* (5. Aufl.). *Grundlagentexte Methoden*. Beltz Juventa.

Kularatne, T. D., Li, J. & Pitt, D. (2021). On the use of Archimedean copulas for insurance modelling. *Annals of Actuarial Science*, *15*(1), 57–81. https://doi.org/10.1017/S1748499520000147

Kurowicka, D. & Cooke, R. (2006). *Uncertainty analysis with high dimensional dependence modelling*. *Wiley series in probability and statistics*. John Wiley.

Lamnek, S. & Krell, C. (2016). *Qualitative Sozialforschung: Mit Online-Material* (6., überarbeitete Auflage). Beltz.

Layton, R. & Watters, P. A. (2014). A methodology for estimating the tangible cost of data breaches. *Journal of Information Security and Applications*, *19*(6), 321–330. https://doi.org/10.1016/j.jisa.2014.10.012

Liebold, R. & Trinczek, R. (2009). Experteninterview. In S. Kühl, P. Strodtholz & A. Taffertshofer (Hrsg.), *Handbuch Methoden der Organisationsforschung* (S. 32–56). VS Verlag für Sozialwissenschaften. https://doi.org/10.1007/978-3-531-91570-8_3

Lloyd, G. (2020). The business benefits of cyber security for SMEs. *Computer Fraud & Security*, *2020*(2), 14–17. https://doi.org/10.1016/S1361-3723(20)30019-1

Lloyd's. (2015). *A quick guide to cyber risk*. https://www.lloyds.com/news-and-insights/news/a-quick-guide-to-cyber-risk. Zugegriffen: 07.04.2021

MacKenzie, C. A. (2014). Summarizing Risk Using Risk Measures and Risk Indices. *Risk Analysis*, *34*(12), 2143–2162. https://doi.org/10.1111/risa.12220

Maillart, T. & Sornette, D. (2010). Heavy-tailed distribution of cyber-risks. *The European Physical Journal B*, *75*(3), 357–364. https://doi.org/10.1140/epjb/e2010-00120-8

Marotta, A., Martinelli, F., Nanni, S., Orlando, A. & Yautsiukhin, A. (2017). Cyber-insurance survey. *Computer Science Review*, *24*, 35–61. https://doi.org/10.1016/j.cosrev.2017.01.001

Marotta, A. & McShane, M. (2018). Integrating a Proactive Technique Into a Holistic Cyber Risk Management Approach: A Holistic Cyber Risk Management Approach. *Risk Management and Insurance Review*, *21*, 435–452. https://doi.org/10.1111/rmir.12109

Mayring, P. (2015). *Qualitative Inhaltsanalyse: Grundlagen und Techniken* (12. Aufl.). *Beltz Pädagogik*. Beltz.

McAfee. (2020). *The hidden costs of cybercrime.* Report. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf. Zugegriffen: 20.04.2021

McDonough, W. J. (2007). Cyber risk and privacy liability: A click in the right direction? *Journal of Healthcare Risk Management*, *27*(4), 9–12. https://doi.org/10.1002/jhrm.5600270403

McKelvey, R. D. & Zavoina, W. (1975). A statistical model for the analysis of ordinal level dependent variables. *The Journal of Mathematical Sociology*, *4*(1), 103–120. https://doi.org/10.1080/0022250X.1975.9989847

McLellan, E., MacQueen, K. M. & Neidig, J. L. (2003). Beyond the Qualitative Interview: Data Preparation and Transcription. *Field Methods*, *15*(1), 63–84. https://doi.org/10.1177/1525822X02239573

McLeod, A. & Dolezel, D. (2018). Cyber-analytics: Modeling factors associated with healthcare data breaches. *Decision Support Systems*, *108*, 57–68. https://doi.org/10.1016/j.dss.2018.02.007

McShane, M. & Nguyen, T. (2020). Time-varying effects of cyberattacks on firm value. *The Geneva Papers on Risk and Insurance - Issues and Practice*, *45*(4), 580–615. https://doi.org/10.1057/s41288-020-00170-x

Meuser, M. & Nagel, U. (2009). The Expert Interview and Changes in Knowledge Production. In A. Bogner, B. Littig & W. Menz (Hrsg.), *Research methods series. Interviewing experts.* Palgrave Macmillan.

Moritz, R. L., Berger, K. M., Owen, B. R. & Gillum, D. R. (2020). Promoting biosecurity by professionalizing biosecurity. *Science*, *367*(6480), 856. https://doi.org/10.1126/science.aba0376

Moshi, M. R., Parsons, J., Tooher, R. & Merlin, T. (2019). Evaluation of mobile health applications: Is regulatory policy up to the challenge? *International Journal of Technology Assessment in Health Care*, *35*(4), 351–360. https://doi.org/10.1017/S0266462319000461

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A. & Sadhukhan, S. K. (2013). Cyber-risk decision models: To insure IT or not? *Decision Support Systems*, *56*, 11–26. https://doi.org/10.1016/j.dss.2013.04.004

Munich Re. (2022). *Munich Re Global Cyber Risk and Insurance Survey*. https://www.munichre.com/topics-online/de/digitalisation/cyber/munich-re-global-cyber-risk-and-insurance-survey.html. Zugegriffen: 16.01.2023

Myers, M. D. (2020). *Qualitative research in business & management* (Third edition). SAGE.

Myers, M. D. & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and Organization*, *17*(1), 2–26. https://doi.org/10.1016/j.infoandorg.2006.11.001

National Conference of State Legislatures (NCSL). (2016). *Security Breach Notification Laws*. https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx. Zugegriffen: 15.02.2022

Nelsen, R. B. (2006). *An Introduction to Copulas* (2. Aufl.). *Springer series in statistics*. Springer. https://doi.org/10.1007/0-387-28678-0

Neubauer, T. & Heurix, J. (2011). A methodology for the pseudonymization of medical data. *International Journal of Medical Informatics*, *80*(3), 190–204. https://doi.org/10.1016/j.ijmedinf.2010.10.016

Nieuwesteeg, B., Visscher, L. & Waard, B. de (2018). The law and economics of cyber insurance contracts: A case study. *European Review of Private Law*, *26*, 371–420. http://www.kluwerlawonline.com/api/Product/CitationPDFURL?file=Journals\ERPL\ERPL2018027.pdf. Zugegriffen: 20.05.2021

National Institute of Standards and Technology (NIST). (2012). *Guide for conducting risk assessments.* https://doi.org/10.6028/NIST.SP.800-30r1

National Institute of Standards and Technology (NIST). (2017). *Cybersecurity framework manufacturing profile.* NISTIR 8183. NISTIR 8183. https://doi.org/10.6028/NIST.IR.8183.

Njegomir, V. & Marović, B. (2012). Contemporary trends in the global insurance industry. *Procedia - Social and Behavioral Sciences*, *44*, 134–142. https://doi.org/10.1016/j.sbspro.2012.05.013

Nosworthy, J. D. (2000). Implementing Information Security In The 21st Century — Do You Have the Balancing Factors? *Computers & Security*, *19*(4), 337–347. https://doi.org/10.1016/S0167-4048(00)04021-9

Nurse, J., Axon, L., Erola, A., Agrafiotis, I., Goldsmith, M. & Creese, S. (2020). The Data that Drives Cyber Insurance: A Study into the Underwriting and Claims Processes. In *2020 International conference on cyber situational awareness, data analytics and assessment (CyberSA)*.

Öğüt, H., Raghunathan, S. & Menon, N. (2011). Cyber security risk management: public policy implications of correlated risk, imperfect ability to prove loss, and observability of self-protection. *Risk Analysis*, *31*(3), 497–512. https://doi.org/10.1111/j.1539-6924.2010.01478.x

Osborn, E. & Simpson, A. (2017). On small-scale IT users' system architectures and cyber security: A UK case study. *Computers & Security*, *70*, 27–50. https://doi.org/10.1016/j.cose.2017.05.001

Palsson, K., Gudmundsson, S. & Shetty, S. (2020). Analysis of the impact of cyber events for cyber insurance. *The Geneva Papers on Risk and Insurance - Issues and Practice*, *45*(4), 564–579. https://doi.org/10.1057/s41288-020-00171-w

Paté-Cornell, M.-E., Kuypers, M., Smith, M. & Keller, P. (2018). Cyber Risk Management for Critical Infrastructure: A Risk Analysis Model and Three Case Studies. *Risk analysis: an official publication of the Society for Risk Analysis*, *38*(2), 226–241. https://doi.org/10.1111/risa.12844

Peng, C., Xu, M., Xu, S. & Hu, T. (2016). Modeling and predicting extreme cyber attack rates via marked point processes. *Journal of Applied Statistics*, *44*(14), 2534–2563. https://doi.org/10.1080/02664763.2016.1257590

Peng, C., Xu, M., Xu, S. & Hu, T. (2018). Modeling multivariate cybersecurity risks. *Journal of Applied Statistics*, *45*(15), 2718–2740. https://doi.org/10.1080/02664763.2018.1436701

Pfleeger, S. L. & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security*, *31*(4), 597–611. https://doi.org/10.1016/j.cose.2011.12.010

Pohlmann, N. (2019). IT-Sicherheit im Krankenhaus: Ohne Cybersicherheit gelingt keine nachhaltige Digitalisierung. *kma - Klinik Management aktuell*, *24*(10), 55–59. https://doi.org/10.1055/s-0039-1700424

Pooser, D. M., Browne, M. J. & Arkhangelska, O. (2018). Growth in the Perception of Cyber Risk: Evidence from U.S. P&C Insurers. *The Geneva Papers on Risk and Insurance - Issues and Practice*, *43*(2), 208–223. https://doi.org/10.1057/s41288-017-0077-9

Poyraz, O. I., Canan, M., McShane, M., Pinto, C. A. & Cotter, T. S. (2020). Cyber assets at risk: monetary impact of U.S. personally identifiable information mega data breaches. *The Geneva Papers on Risk and Insurance - Issues and Practice*, *45*(4), 616–638. https://doi.org/10.1057/s41288-020-00185-4

Priestman, W., Anstis, T., Sebire, I. G., Sridharan, S. & Sebire, N. J. (2019). Phishing in healthcare organisations: threats, mitigation and approaches. *BMJ Health & Care Informatics*, *26*(1). https://doi.org/10.1136/bmjhci-2019-100031

Rakes, T. R., Deane, J. K. & Paul Rees, L. (2012). IT security planning under uncertainty for high-impact events. *Omega*, *40*(1), 79–88. https://doi.org/10.1016/j.omega.2011.03.008

Randolph, J. (2009). A Guide to Writing the Dissertation Literature Review. *Practical Assessment, Research, and Evaluation*, *14*(13). https://doi.org/10.7275/B0AZ-8T74

Refsdal, A., Stølen, K. & Solhaug, B. (2015). *Cyber-risk management*. *SpringerBriefs in computer science*. Springer. https://doi.org/10.1007/978-3-319-23570-7

Robert, C. P. & Casella, G. (2004). *Monte Carlo Statistical Methods*. Springer New York. https://doi.org/10.1007/978-1-4757-4145-2

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, *2*(2), 121-135. https://doi.org/10.1093/cybsec/tyw001

Romanosky, S., Ablon, L., Kuehn, A. & Jones, T. (2019). Content analysis of cyber insurance policies: how do carriers price cyber risk? *Journal of Cybersecurity*, *5*(1), 1–19. https://doi.org/10.1093/cybsec/tyz002

Ruan, K. (2017). Introducing cybernomics: A unifying economic framework for measuring cyber risk. *Computers & Security*, *65*, 77–89. https://doi.org/10.1016/j.cose.2016.10.009

Salmela, H. (2008). Analysing Business Losses Caused by Information Systems Risk: A Business Process Analysis Approach. *Journal of Information Technology*, *23*(3), 185–202. https://doi.org/10.1057/palgrave.jit.2000122

Samhan, B. (2017). Can cyber risk management insurance mitigate healthcare providers' intentions to resist electronic medical records? *International Journal of Healthcare Management*, *13*(1), 12–21. https://doi.org/10.1080/20479700.2017.1412558

Sardi, A., Rizzi, A., Sorano, E. & Guerrieri, A. (2020). Cyber Risk in Health Facilities: A Systematic Literature Review. *Sustainability*, *12*(17), 7002. https://doi.org/10.3390/su12177002

Schmitz, R.-M. & Pedell, B. (2013). Steuerung eines Krankenhauses der Maximalversorgung. *Controlling*(2), 121–124. https://doi.org/10.15358/0935-0381_2013_2_121

Schnell, R., Hill, P. B. & Esser, E. (2018). *Methoden der empirischen Sozialforschung* (11. Aufl.). *De Gruyter Studium*. De Gruyter Oldenbourg.

Seibold, H. (2006). *IT-Risikomanagement*. De Gruyter. https://doi.org/10.1524/9783486840346

Sheehan, B., Murphy, F., Kia, A. N. & Kiely, R. (2021). A quantitative bow-tie cyber risk classification and assessment framework. *Journal of Risk Research*, *24*(12), 1619–1638. https://doi.org/10.1080/13669877.2021.1900337

Shetty, S., McShane, M., Zhang, L., Kesan, J. P., Kamhoua, C. A., Kwiat, K. & Njilla, L. L. (2018). Reducing Informational Disadvantages to Improve Cyber Risk Management. *The Geneva Papers on Risk and Insurance - Issues and Practice*, *43*(2), 224–238. https://doi.org/10.1057/s41288-018-0078-3

Shi, P. & Yang, L. (2018). Pair Copula Constructions for Insurance Experience Rating. *Journal of the American Statistical Association*, *113*(521), 122–133. https://doi.org/10.1080/01621459.2017.1330692

Shoffner, M., Owen, P., Mostafa, J., Lamm, B., Wang, X., Schmitt, C. P. & Ahalt, S. C. (2013). The secure medical research workspace: An IT infrastructure to enable secure research on clinical data. *Clinical and Translational Science*, *6*(3), 222–225. https://doi.org/10.1111/cts.12060

Smidt, G. de & Botzen, W. (2018). Perceptions of Corporate Cyber Risks and Insurance Decision-Making. *The Geneva Papers on Risk and Insurance - Issues and Practice*, *43*(2), 239–274. https://doi.org/10.1057/s41288-018-0082-7

Smith, G. S. (2004). Recognizing and Preparing Loss Estimates from Cyber-Attacks. *Information Systems Security*, *12*(6), 46–57. https://doi.org/10.1201/1086/44022.12.6.20040101/79786.8

Smith, M. S. (2015). Copula modelling of dependence in multivariate time series. *International Journal of Forecasting*, *31*(3), 815–833. https://doi.org/10.1016/j.ijforecast.2014.04.003

Smith, E. & Eloff, J. (1999). Security in health-care information systems—current trends. *International Journal of Medical Informatics*, *54*(1), 39–54. https://doi.org/10.1016/S1386-5056(98)00168-3

Smith, G. E., Watson, K. J., Baker, W. H. & Pokorski II, J. A. (2007). A critical balance: collaboration and security in the IT-enabled supply chain. *International Journal of Production Research*, *45*(11), 2595–2613. https://doi.org/10.1080/00207540601020544

Solms, R. von & Niekerk, J. van (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Sonnenreich, W., Albanese, J. & Stout, B. (2006). Return on security investment (ROSI) - A practical quantitative model. *Journal of Research and Practice in Information Technology*, *38*(1), 45–56. https://doi.org/10.5220/0002580202390252

Statista. (2022). *Estimated cost of cybercrime globally 2016-2027*. https://www.statista.com/statistics/1280009/cost-cybercrime-worldwide/. Zugegriffen: 21.01.2023

Strupczewski, G. (2021). Defining cyber risk. *Safety Science*, *135*, 105143. https://doi.org/10.1016/j.ssci.2020.105143

Sturm, P. (2013). Operational and reputational risk in the European banking industry: The market reaction to operational risk events. *Journal of Economic Behavior & Organization*, *85*, 191–206. https://doi.org/10.1016/j.jebo.2012.04.005

Tavabi, N., Abeliuk, A., Mokhberian, N., Abramson, J. & Lerman, K. (2020). Challenges in Forecasting Malicious Events from Incomplete Data. In A. E. F. Seghrouchni (Hrsg.), *ACM Digital Library, Companion Proceedings of the Web Conference 2020* (S. 603–610). Association for Computing Machinery. https://doi.org/10.1145/3366424.3385774

Taylor, H., Artman, E. & Woelfer, J. P. (2012). Information Technology Project Risk Management: Bridging the Gap between Research and Practice. *Journal of Information Technology*, *27*(1), 17–34. https://doi.org/10.1057/jit.2011.29

Thomson, M. E. & Solms, R. von (1998). Information security awareness: educating your users effectively. *Information Management & Computer Security*, *6*(4), 167–173. https://doi.org/10.1108/09685229810227649

Tsohou, A., Karyda, M., Kokolakis, S. & Kiountouzis, E. (2012). Analyzing trajectories of information security awareness. *Information Technology & People*, *25*(3), 327–352. https://doi.org/10.1108/09593841211254358

Tully, J., Selzer, J., Phillips, J. P., O'Connor, P. & Dameff, C. (2020). Healthcare Challenges in the Era of Cybersecurity. *Health security*, *18*(3), 228–231. https://doi.org/10.1089/hs.2019.0123

Wangen, G., Hallstensen, C. & Snekkenes, E. (2018). A framework for estimating information security risk assessment method completeness. *International Journal of Information Security*, *17*(6), 681–699. https://doi.org/10.1007/s10207-017-0382-0

Webb, T. & Dayal, S. (2017). Building the wall: Addressing cybersecurity risks in medical devices in the U.S.A. and Australia. *Computer Law & Security Review*, *33*(4), 559–563. https://doi.org/10.1016/j.clsr.2017.05.004

World Economic Forum (WEF). (2012). *Partnering for cyber resilience: Risk and responsibility in a hyperconnected world - Principles and guidelines*. http://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf. Zugegriffen: 07.04.2021

World Economic Forum (WEF). (2016). *Understanding systemic cyber risk: Global agenda council on risk & resilience.* White Paper. http://www3.weforum.org/docs/White_Paper_GAC_Cyber_Resilience_VERSION_2.pdf. Zugegriffen: 07.04.2021

World Economic Forum (WEF). (2021). *The global risks report 2021: 16th edition. Insight report*. http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf. Zugegriffen: 10.05.2021

World Economic Forum (WEF). (2023). *The global risks report 2023: 18th edition. Insight report*. https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf. Zugegriffen: 13.02.2023

Wheatley, S., Hofmann, A. & Sornette, D. (2021). Addressing insurance of data breach cyber risks in the catastrophe framework. *The Geneva Papers on Risk and Insurance - Issues and Practice*, *46*(1), 53–78. https://doi.org/10.1057/s41288-020-00163-w

Wheatley, S., Maillart, T. & Sornette, D. (2016). The extreme risk of personal data breaches and the erosion of privacy. *The European Physical Journal B*, *89*(1). https://doi.org/10.1140/epjb/e2015-60754-4

Whitman, M. & Mattord, H. (2014). Information Security Governance for the Non-security Business Executive. *Journal of Executive Education*, *11*, 97–111.

Williams, P. & Woodward, A. (2015). Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem. *Medical Devices: Evidence and Research*, *8*, 305–316. https://doi.org/10.2147/MDER.S50048

Willis Tower Watson (2013). Willis report: Majority of Public Companies Indicate Cyber Attack Would Cause "Serious Harm" or "Adversely Impact" Their Firms. Willis Towers Watson, London.

Witte, A.-K., Fuerstenau, D. & Zarnekow, R. (2020). *Digital Health Ecosystems for Sensor Technology Integration - A Qualitative Study on the Paradox of Data Openness*. Hyderabad, India. 41st International Conference on Information Systems (ICIS) 2020.

Woods, D. W. & Böhme, R. (2021). Systematization of Knowledge: Quantifying Cyber Risk. *IEEE Symposium on Security & Privacy*. https://informationsecurity.uibk.ac.at/pdfs/WB2020_sok_cyberrisk_snp.pdf. Zugegriffen: 19.04.2021

Wozak, F., Schabetsberger, T. & Ammmenwerth, E. (2007). End-to-end security in telemedical networks – A practical guideline. *International Journal of Medical Informatics*, *76*(5), 484–490. https://doi.org/10.1016/j.ijmedinf.2006.09.020

Wrede, D., Freers, T. & Graf von der Schulenburg, J.-M. (2018). Herausforderungen und Implikationen für das Cyber-Risikomanagement sowie die Versicherung von Cyberrisiken – Eine empirische Analyse. *Zeitschrift für die gesamte Versicherungswissenschaft*, *107*(4), 405–434. https://doi.org/10.1007/s12297-018-0425-2

Wu, M. Z., Luo, J., Fang, X., Xu, M. & Zhao, P. (2021). Modeling multivariate cyber risks: deep learning dating extreme value theory. *Journal of Applied Statistics*, 1–21. https://doi.org/10.1080/02664763.2021.1936468z

Xie, X., Lee, C. & Eling, M. (2020). Cyber insurance offering and performance: an analysis of the U.S. cyber insurance market. *The Geneva Papers on Risk and Insurance - Issues and Practice*, *45*(4), 690–736. https://doi.org/10.1057/s41288-020-00176-5

Xu, M., Schweitzer, K. M., Bateman, R. M. & Xu, S. (2018). Modeling and Predicting Cyber Hacking Breaches. *IEEE Transactions on Information Forensics and Security*, *13*(11), 2856–2871. https://doi.org/10.1109/TIFS.2018.2834227

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6. Aufl.). SAGE.

Zängerle, D. & Schiereck, D. (2023a). Cyberrisiken – Vom Begriffswirrwarr zu einem einheitlichen Begriffsverständnis. *HMD Praxis der Wirtschaftsinformatik*, *60*(1), 214–229. https://doi.org/10.1365/s40702-022-00888-3

Zängerle, D. & Schiereck, D. (2023b). Modelling and predicting enterprise-level cyber risks in the context of sparse data availability. *The Geneva Papers on Risk and Insurance - Issues and Practice, 48,* 434–462. https://doi.org/10.1057/s41288-022-00282-6

Zeller, G. & Scherer, M. (2021). A comprehensive model for cyber risk based on marked point processes and its application to insurance. *European Actuarial Journal.* https://doi.org/10.1007/s13385-021-00290-1

Zhao, Z., Shi, P. & Zhang, Z. (2020). Modeling Multivariate Time Series With Copula-Linked Univariate D-Vines. *Journal of Business & Economic Statistics*, 1–15. https://doi.org/10.1080/07350015.2020.1859381