Forum V-Versicherungsmathematisches Kolloquium

Cyber-Risk & Cyber-Governance – von neuen Geschäftsfeldern und regulatorischen Herausforderungen

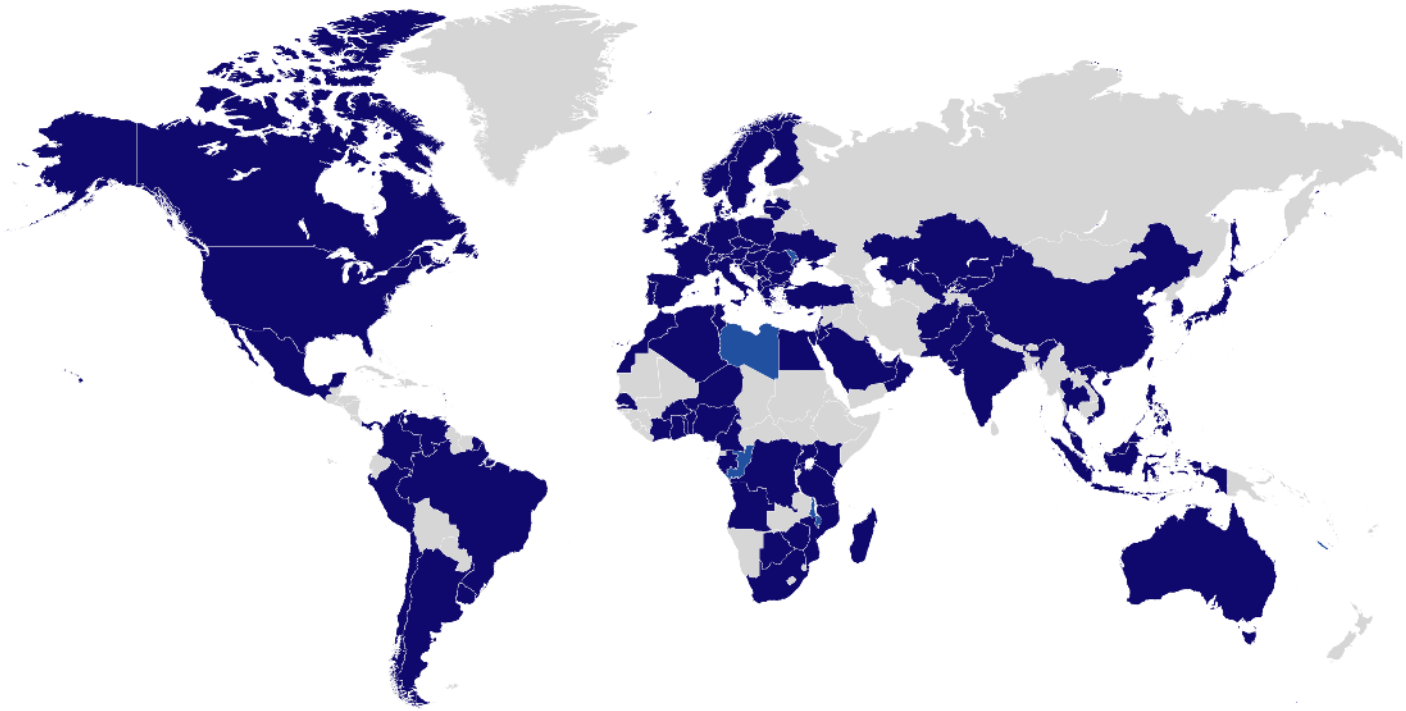
9. Juli 2024 – Digitale Veranstaltung (17:15 – 18:45)

forvis mazars

Forvis Mazars für Forum V – Versicherungsmathematisches Kolloquium

Wer wir sind

Forvis Mazars ist ein weltweit führendes Professional Services-Netzwerk. Unser Team mit mehr als 40.000 Professionals verbindet das Commitment, weltweit eine Unmatched Client Experience zu bieten.



Stand: 1. Juni 2024

- Forvis Mazars
- Korrespondenten der Forvis Mazars Gruppe

Forvis Mazars ist der Brand-Name des Forvis Mazars Global Network (Forvis Mazars Global Limited) und der beiden unabhängigen Mitglieder: Forvis Mazars, LLP in den Vereinigten Staaten und Forvis Mazars Group SC, einer international integrierten Partnerschaft, die in über 100 Ländern und Regionen tätig ist.

- Afghanistan
- Ägypten
- Albanien
- Algerien
- Angola
- Argentinien
- Australien
- Bahrain
- Belgien
- Benin
- Bermuda
- Bosnien und Herzegowina
- Botswana
- Brasilien
- Bulgarien
- Burkina Faso
- Chile
- China
- Dänemark
- Demokratische Republik Kongo (DRK)
- Deutschland
- Elfenbeinküste
- Finnland
- Frankreich
- Gabun
- Ghana
- Griechenland
- Hongkong (SAR)
- Indien
- Indonesien
- Irland
- Israel
- Italien
- Japan
- Jordanien
- Kaimaninseln
- Kamerun
- Kanada
- Kasachstan
- Katar
- Kenia
- Kirgisistan
- Kolumbien
- Kongo
- Korea
- Kosovo
- Kroatien
- Kuwait
- Lettland
- Libanon
- Libyen
- Litauen
- Luxemburg
- Madagaskar
- Malawi
- Malaysia
- Malta
- Marokko
- Mauritius
- Mexiko
- Moldau
- Mosambik
- Neukaledonien
- Niederlande
- Niger
- Nigeria
- Nordmazedonien
- Norwegen
- Österreich
- Oman
- Pakistan
- Palästina
- Panama
- Peru
- Philippinen
- Polen
- Portugal
- Ruanda
- Rumänien
- Saudi-Arabien
- Schweden
- Schweiz
- Senegal
- Serbien
- Simbabwe
- Singapur
- Slowakei
- Slowenien
- Spanien
- Südafrika
- Taiwan
- Tansania
- Thailand
- Togo
- Tschechische Republik
- Tunesien
- Türkei
- Uganda
- Ukraine
- Ungarn
- Uruguay
- USA
- Usbekistan
- Venezuela
- Vereinigte Arabische Emirate
- Vereinigtes Königreich
- Vietnam
- Zypern

Forvis Mazars für Forum V – Versicherungsmathematisches Kolloquium

Heute bei Ihnen

Meinolf List

Senior Manager
OneInsurance Forvis Mazars
München

meinolf.list@mazars.de
+49 170 3766 252

- Versicherungsmathematiker mit Fokus auf Bilanzierung und Modellierung von Lebens- und Krankenversicherungsprodukten
- Schwerpunkte im Bereich der Regulierung und Bilanzierung von Einrichtungen der betrieblichen Altersvorsorge (Pensionskassen, Pensionsfonds, Unterstützungskassen) sowie Versorgungswerken
- Aktuarielle Reservierung im Kontext von HGB, Solvency II und IFRS17
- Aktuarielles (aufsichtsrechtliches) Reporting
- Gastvorträge Forum V /
  Nordbay. Institut für Versicherungswissenschaft und –wirtschaft:
  - Aktuelle Emerging Risks und deren Effekt auf die Versicherungsbranche
  - Herausforderungen der Versicherungsbranche für die Governance

Alexandre Extrat

Aktuar (DAV)
Manager
OneInsurance Forvis Mazars
Köln

alexandre.extrat@mazars.de
+49 170 3754 391

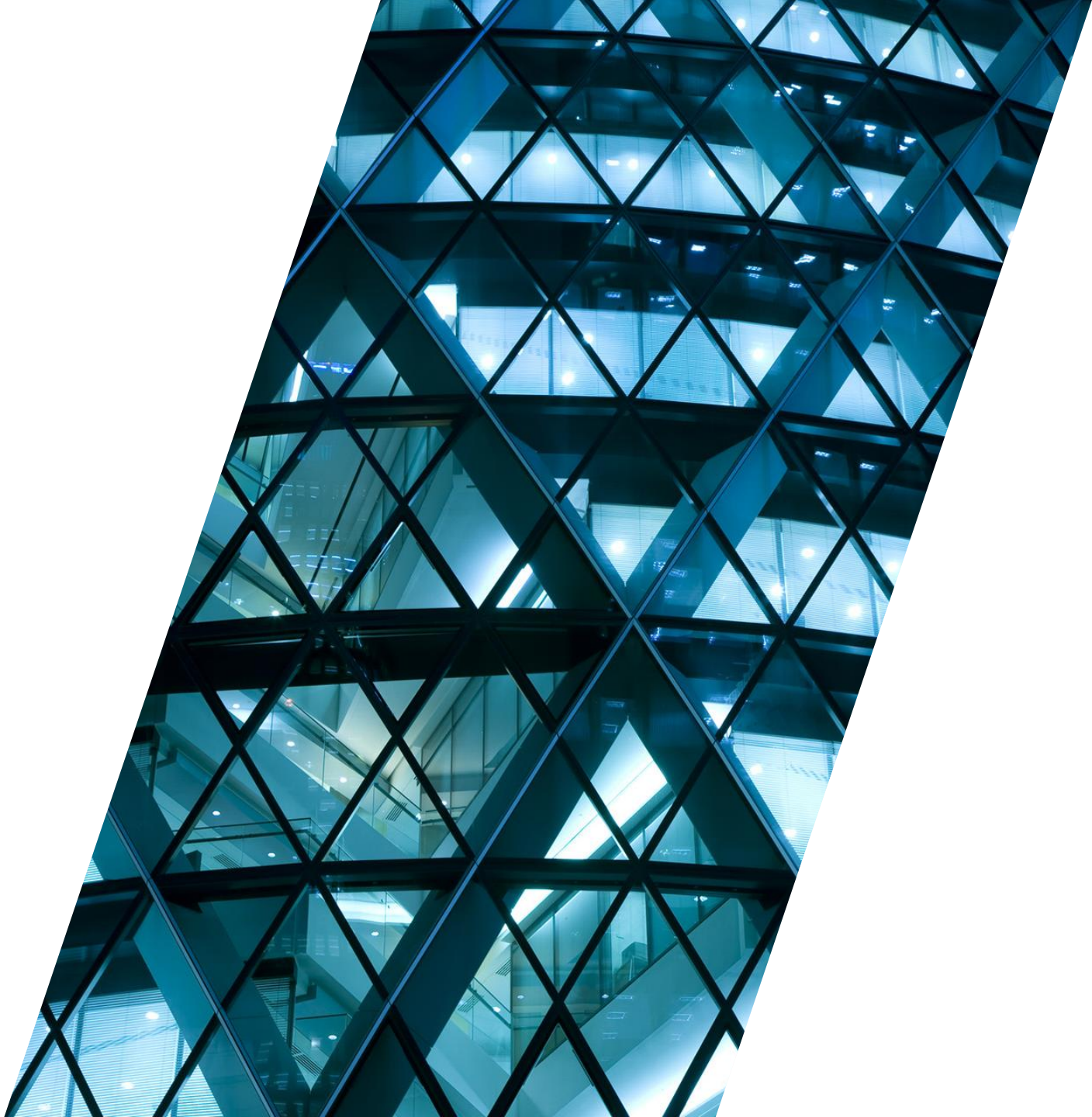
- Aktuar (DAV) mit Schwerpunkt auf Projektionsmodelle und aktuarielle Cash-Flow-Modellierung
- Aktuarielle Reservierung für Solvency II und IFRS17 als Berater und Prüfer für nationale und internationale Versicherungsgruppen
- Modellierungsexperte für Lebens- und Krankenversicherungstarife
- Cyber- und ESG-Experte im Rahmen der aktuariellen Modellierung und Projektion zugehöriger Risikomaße
- Kapitalmarktpfadmodellierung / ESG-Szenarioentwicklung und Illiquidity Adjustment Validierung
- Aktuarielles (aufsichtsrechtliches) Reporting

Agenda

1. Überblick Emerging Risk Cyberrisiko
2. Regulatorische Aspekte Cyberrisiken Versicherungensbranche
    1. Überblick über Regulierung und Governance
    2. DORA-Verordnung / FinmadiG
3. Herausforderung für die Modellierung
4. Ausblick und Zusammenfassung

01

Überblick Emerging Risk Cyberrisiko



Cyber-Risk & Cyber-Governance – von neuen Geschäftsfeldern…
Überblick Emerging Risk Cyberrisiko

Wie definiert sich ein Cyberrisiko und die Cybersicherheit?

GDV Gesamtverband der Versicherer

DAV
DEUTSCHE AKTUARVEREINIGUNG e.V.

Ein Cyberrisiko stellt das Risiko **jeglicher Verletzung der Informationssicherheit** dar. Informationssicherheit umfasst dabei die uneingeschränkte Verfügbarkeit von Systemen und Daten sowie die Gewährleistung der Vertraulichkeit und Integrität der Daten.

Quelle: https://aktuar.de/unsere-themen/fachgrundsaetze-oeffentlich/DAV_AGCyber-Ergebnisbericht_.pdf

eiopa
European Insurance and Occupational Pensions Authority

„Cyber risk can be defined as any type of risk emanating from the **use of electronic data** and **its transmission**, including technology tools such as the internet and telecommunications networks. It also **encompasses physical damage** that can be caused by cybersecurity incidents, **fraud** committed by misuse of data, any **liability arising from data storage**, and the **availability, integrity and confidentiality of electronic information** − being related to individuals, companies, or governments.“

Quelle: https://aktuar.de/unsere-themen/fachgrundsaetze-oeffentlich/DAV_AGCyber-Ergebnisbericht_.pdf

forvis mazars

Cyber-Risk & Cyber-Governance – von neuen Geschäftsfeldern…
Überblick Emerging Risk Cyberrisiko

Wie definiert sich ein Cyberrisiko und die Cybersicherheit?

Europäische Union

„Cyberbedrohung“ bezeichnet einen möglichen Umstand, ein mögliches Ereignis oder eine mögliche Handlung, der/das/die Netz- und Informationssysteme, die Nutzer dieser Systeme und andere Personen schädigen, stören oder anderweitig beeinträchtigen könnte.“

Quelle: Verordnung (EU) 2019/881
Verordnung über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik

Cyber-Risk & Cyber-Governance – von neuen Geschäftsfeldern…
Überblick Emerging Risk Cyberrisiko

Wie definiert sich ein Cyberrisiko und die Cybersicherheit?

Risikoeinteilung

Klassische Risiken = nicht Emerging Risks	**Emerging Risk**	**Nicht versicherbare Risken**
„Alles, was bekannt ist und schonmal erlebt worden ist“ – Tod – Berufsunfähigkeit (bekannt) – Bekannte Krankheiten – Sachschäden (ohne Nuklearschäden)	Generell werden drei Typen* von Emerging Risks unterschieden: I. Neues Risiko in bekannter Risikoexposition II. Ein bekanntes Risiko in neuer Ausprägung III. Neues Risiko mit neuer Ausprägung *Hopkin, P. (2018) Fundamentals of Risk Management: Understanding, evaluating and implementing effective risk management. 5th edition. IRM. Kogan Page: New York.	Alles, was nicht klassisch oder Emerging Risk ist – Armut – Kriminalität – Krieg – …. ***Leseempfehlung:** „Large Risks and Limits of Insurability“ von Baruch Berliner, Geneva Papers on Risk and Insurance Vo. 10, No. 37, Oct. 1985, pp. 313-329

Cyber-Risk & Cyber-Governance – von neuen Geschäftsfeldern…
Überblick Emerging Risk Cyberrisiko

Wie definiert sich ein Cyberrisiko und die Cybersicherheit?

Emerging Risk Klassifizierung	Beispiele	Eigenschaften des Beispiels
I. Neues Risiko in bekannter Risikoexposition	**Cyberrisiken** Datendiebstahl, Identitätsverlust	Das Entwenden von Eigentum ist seit jeher bekannt (Risikoexposition); die Erkenntnis, dass persönliche Daten ein Eigentum darstellen, ist „relativ“ neu.
II. Ein bekanntes Risiko in neuer Ausprägung	**Klimarisiken (regional)** Tornados in Deutschland, Flut im Ahrtal, Abschmelzen der Gletscher	Das Risiko von Unwetter ist seit jeher bekannt, die Exposition in Deutschland durch den Klimawandel erreicht jedoch neue Ausprägungen.
III. Neues Risiko mit neuer Ausprägung	**Entwicklung / Einsatz Künstlicher Intelligenz**	Wurde noch nie erlebt und kann bis zum Eintreten nicht abgeschätzt werden.

Cyber-Risk & Cyber-Governance – von neuen Geschäftsfeldern…
Überblick Emerging Risk Cyberrisiko

Wie definiert sich ein Cyberrisiko und die Cybersicherheit?

Charakterisierung Emerging Risks

Folgende Eigenschaften zeichnen Emerging Risks aus

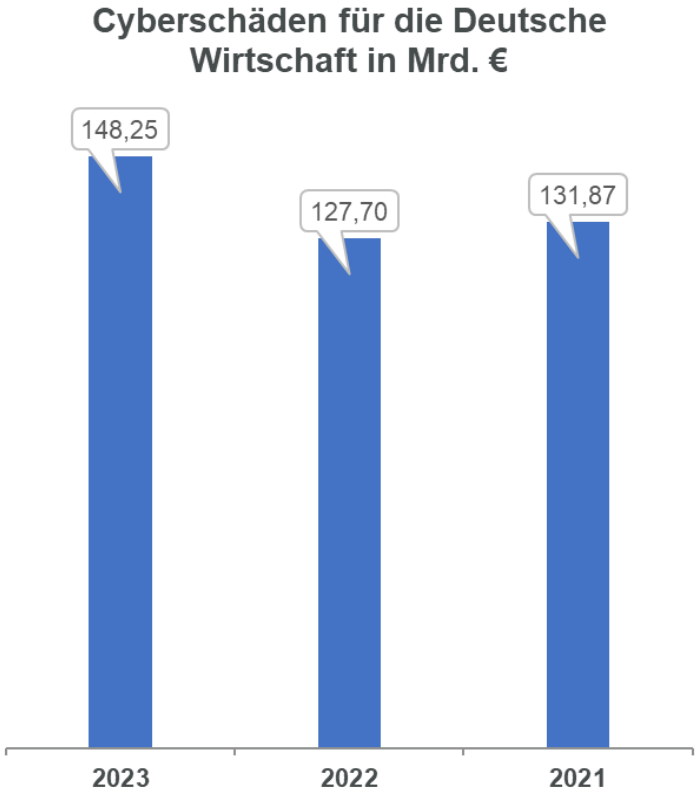
1. Komplex → Verzweigte Abhängigkeiten
2. Unsicher → Fehlende Erfahrung erschwert Abschätzung
3. Chaotisch → Laufende Veränderung zeichnen ER aus
4. Volatil → aus 1. bis 3. ergeben sich Wechselwirkungen
5. Wesentlich → Potenzial zu gewaltigem Schadenausmaß

6. Extern → Steuerung nicht möglich / Reaktion selten Aktion
7. Temporär → ER werden zum „normalen“ Risiko, wenn sie verstanden werden

Emerging Risks bedürfen kein Schadenereignis, um als ER klassifiziert zu werden.
Das Potenzial alleine ist ausreichend

Cyber-Risk & Cyber-Governance – von neuen Geschäftsfeldern…
Überblick Emerging Risk Cyberrisiko

Cyberrisiko und Cyberversicherungsmarkt in Zahlen (1/3)



bitkom

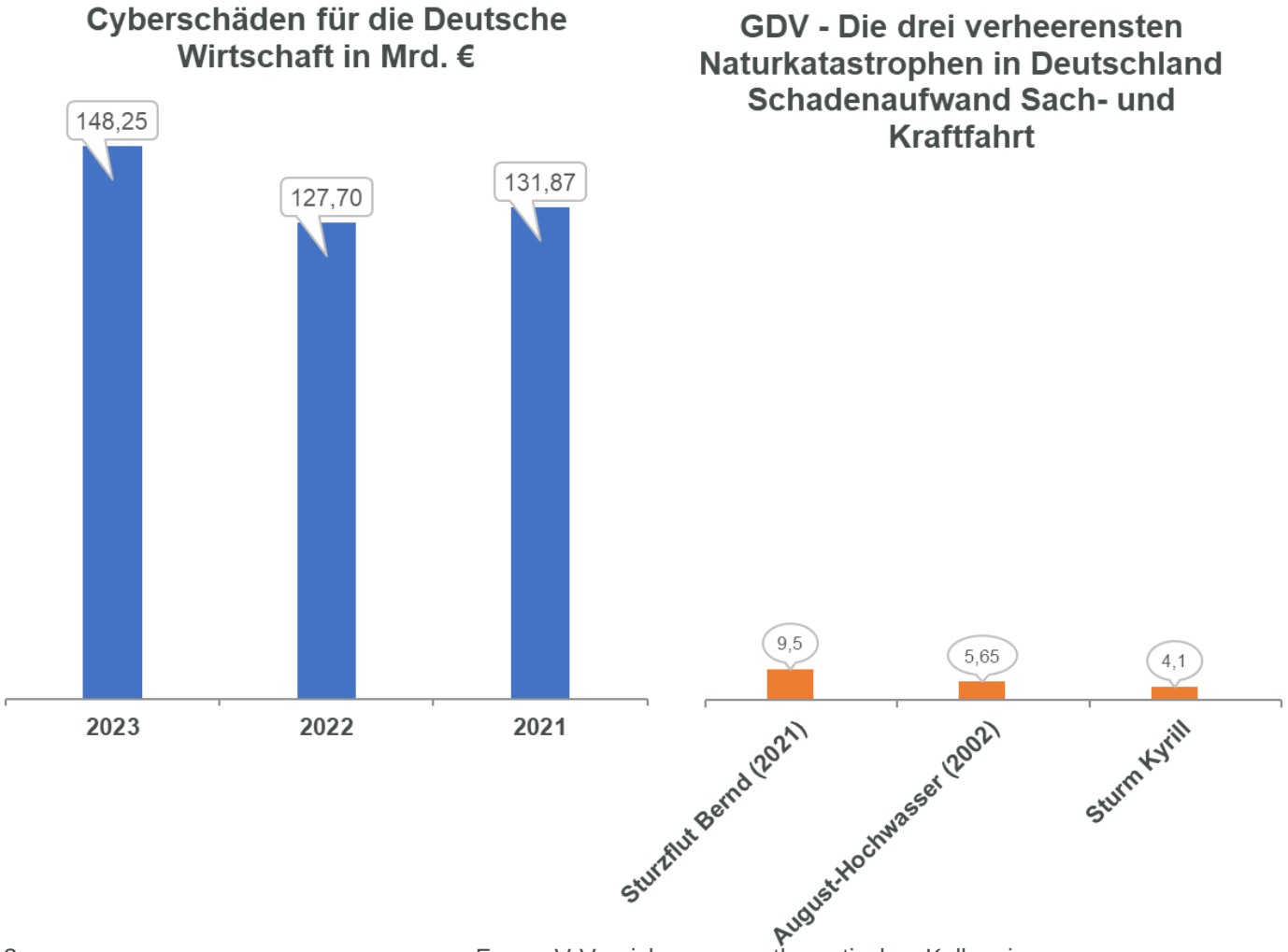
Die Bitkom-Gruppe | Bitkom e. V.

Wirtschaftsschutzbericht 2023 des Branchenverbandes bitkom e.V. veröffentlicht Zahlen zu Cyberschäden und Informationssicherheit.

Befragt wurden Unternehmen in Deutschland mit mindestens zehn Beschäftigten und einem Jahresumsatz von 1 Mio. Euro oder mehr.

Cyber-Risk & Cyber-Governance – von neuen Geschäftsfeldern…
Überblick Emerging Risk Cyberrisiko

Cyberrisiko und Cyberversicherungsmarkt in Zahlen (2/3)



bitkom

Die Bitkom-Gruppe | Bitkom e. V.

Wirtschaftsschutzbericht 2023 des Branchenverbandes bitkom e.V. veröffentlicht Zahlen zu Cyberschäden und Informationssicherheit.

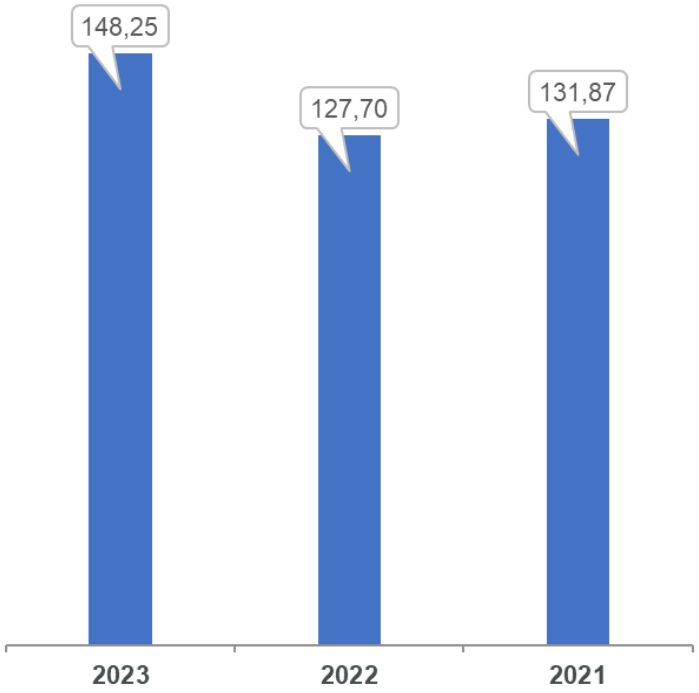
Befragt wurden Unternehmen in Deutschland mit mindestens zehn Beschäftigten und einem Jahresumsatz von 1 Mio. Euro oder mehr.

forvis mazars

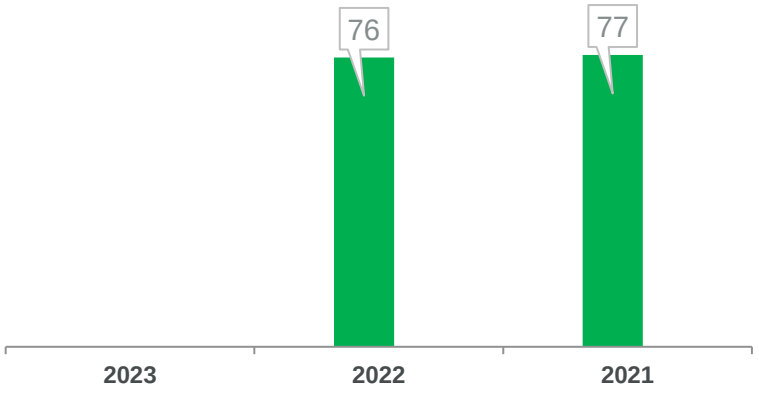
Cyber-Risk & Cyber-Governance – von neuen Geschäftsfeldern…
Überblick Emerging Risk Cyberrisiko

Cyberrisiko und Cyberversicherungsmarkt in Zahlen (3/3)

Cyberschäden für die Deutsche Wirtschaft in Mrd. €



BaFin Statistik - Ausgewählte Posten der GuV für Schaden- und Unfallversicherungsunternehmen Brutto-Aufwendungen für Versicherungsfälle des GJ



bitkom

Die Bitkom-Gruppe | Bitkom e. V.

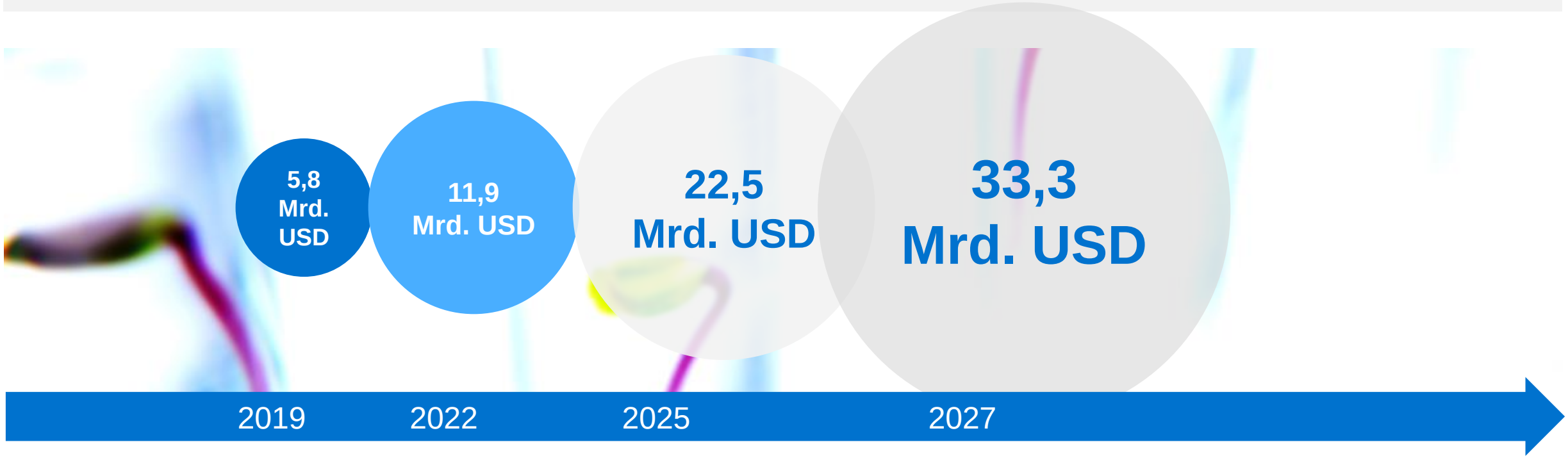
Wirtschaftsschutzbericht 2023 des Branchenverbandes bitkom e.V. veröffentlicht Zahlen zu Cyberschäden und Informationssicherheit.

Befragt wurden Unternehmen in Deutschland mit mindestens zehn Beschäftigten und einem Jahresumsatz von 1 Mio. Euro oder mehr.

Cyber-Risk & Cyber-Governance – von neuen Geschäftsfeldern…
Überblick Emerging Risk Cyberrisiko

Cyberrisiko und Cyberversicherungsmarkt in Zahlen (Ausblick Geschäftsentwicklung)

Die Münchener Rückversicherungsgesellschaft AG schätzt, dass der weltweite Bedarf an Versicherungsschutz für Cyberrisiken bis zum Jahr 2027 ein Volumen von **33,3 Milliarden US-Dollar** erreichen könnte.



https://www.munichre.com/landingpage/en/cyber-insurance-risks-and-trends-2023.html

Cyber-Risk & Cyber-Governance – von neuen Geschäftsfeldern…
Überblick Emerging Risk Cyberrisiko

Trendeinschätzung

	AXA Report 2023 GER	AXA Report 2023 Global	Munich Re Tech Trend Radar 2023	Allianz Risk Barometer 2024	World Economic Forum / Global Risk Report
Nr. 1	Klimawandel	Climate Change	Redefining Industries	**Cyber-Vorfälle**	Klimawandel**
Nr. 2	Geopolitische Instabilität	**Cyber Security Risk**	**Cyber & Crypto**	Betriebs-unterbrechungen	Migration
Nr. 3	**Cyberrisiken**	Geopolitical Instability	Data & AI	Naturkatastrophen	Ressourcen-engpässe
Nr. 4	Gesellschaftliche Spannungen	Risk related to AI	Connected Experience	Gesetzliche / Regulatorische Änderungen	Soziale Disruption
Nr. 5	Biodiversität	Energy Risks	Healthy Human	Makroökonomische Entwicklung	**Cyberkriminalität**

https://commercial.allianz.com/news-and-insights/reports/allianz-risk-barometer.html#download

https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf

https://www.axa.de/presse/mediathek/studien-und-forschung/future-risks-report-2023

https://www.munichre.com/content/dam/munichre/contentlounge/website-pieces/documents/Tech-Trend-Radar-2023-Presentation.pdf/_jcr_content/renditions/original./Tech-Trend-Radar-2023-Presentation.pdf

Cyber-Risk & Cyber-Governance – von neuen Geschäftsfeldern…

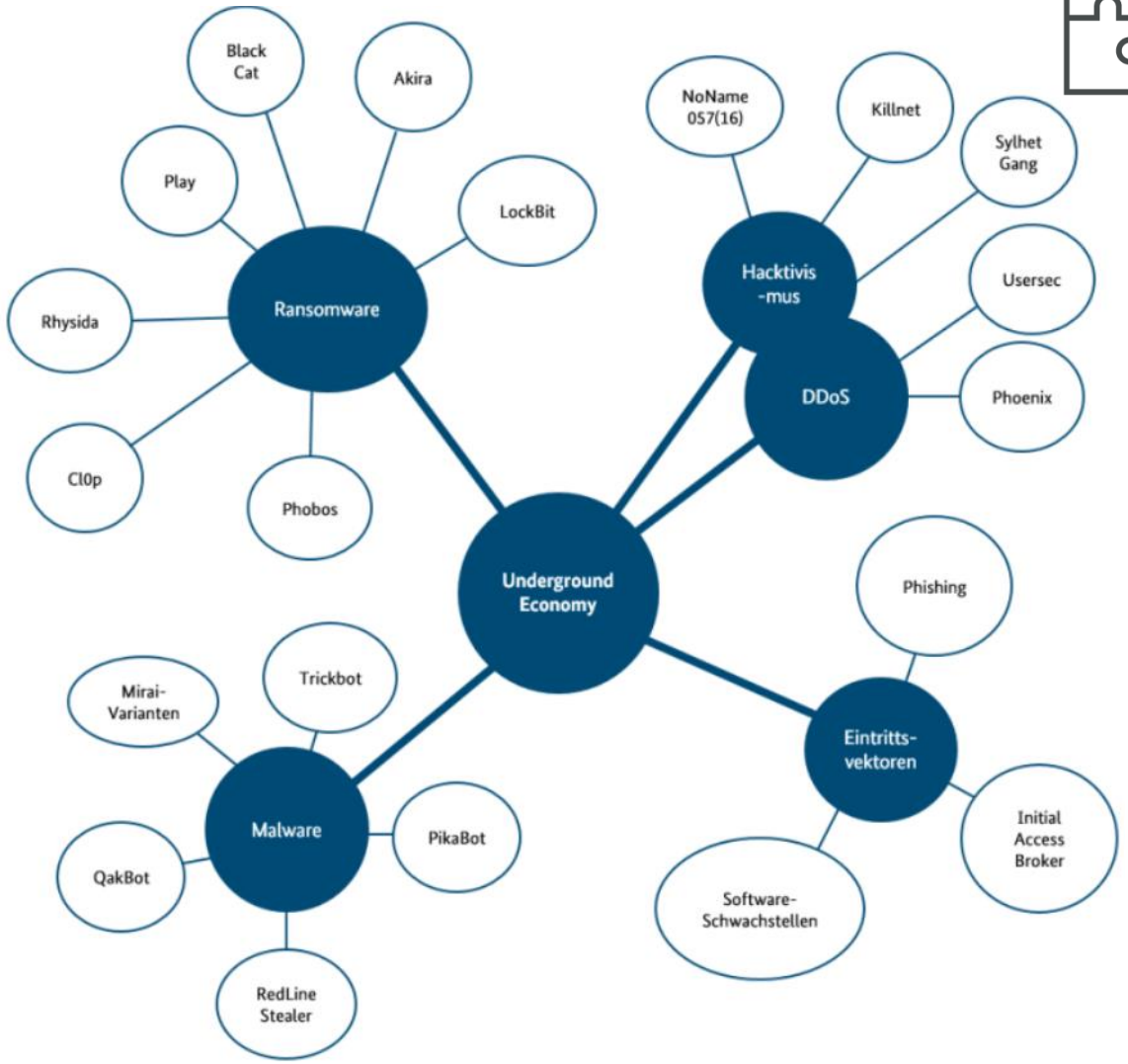
Überblick Emerging Risk Cyberrisiko

Methoden der Cyberbedrohung

Bundeskriminalamt

Die Ziele von cyberkriminellen Akteuern sind äußert vierlfältig. Neben finanzstarken Unternehmen standen auch Einrichtungen und Institutionen mit hoher Öffentlichkeitswirksamkeit im Fokus. Aber auch leicht verwundbare kleine und mittelständige Unternehmen waren aufgrund des opportunistischen Vorgehens der Täter stark betroffen.

Insgesamt war die hohe Bedrohungslage für das Jahr 2023 geprägt von hacktivistischen DDoS-Kampagnen und einer Vielzahl an Ransomware-Angriffen, die teils weitreichende Auswirkungen auf IT-Supply-Chains hatten.



https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2023.html?nn=28110
05.07.2024 / 15:00

Cyber-Risk & Cyber-Governance – von neuen Geschäftsfeldern…
Überblick Emerging Risk Cyberrisiko

Methoden der Cyberbedrohung

Cyberbedrohung	Ausprägung	Schadenereignis / -ziel
Schadsoftware	Sammelbegriff für alle Arten schädlicher Software einschließlich Würmern, Ransomware, Spyware und Viren. Das Ziel ist die Schwächung von Computern oder Netzwerken	Dateien verändern / löschen, vertrauliche Daten ausspioniert bzw. schädliche Daten einschleusen
Ransomware	Ransomware ist eine Form der Erpressung, bei der Schadsoftware eingesetzt wird, um Dateien zu verschlüsseln und unbrauchbar zu machen.	Lösegeld
Social Engineering	Beim Social Engineering erschleichen sich Angreifer das Vertrauen der Menschen, um sie zur Herausgabe von Kontodaten oder zum Herunterladen von Schadsoftware zu drängen.	Dateien verändern / löschen, vertrauliche Daten ausspioniert bzw. schädliche Daten einschleusen
Phishing		
Insiderbedrohungen	Bei einer Insiderbedrohung entstehen Sicherheitsverletzungen oder finanzielle Schäden durch Personen, die bereits Zugang zu bestimmten Systemen haben, wie z. B. Mitarbeitende, Auftragnehmer oder Kunden.	
Komplexe anhaltende Bedrohungen	Bei einer komplexen anhaltenden Bedrohung verschaffen sich Angreifer Zugang zu Systemen, wobei sie über einen längeren Zeitraum unentdeckt bleiben. Die Eindringlinge durchforsten die Systeme des Zielunternehmens und stehlen Daten, ohne dass irgendwelche Gegenmaßnahmen ausgelöst werden.	Spionage, Desinformation, (politische) Einflussnahme

Quelle: (28.06.2024 / 16:30) https://www.microsoft.com/de-de/security/business/security-101/what-is-cybersecurity

Cyber-Risk & Cyber-Governance – von neuen Geschäftsfeldern…
Überblick Emerging Risk Cyberrisiko

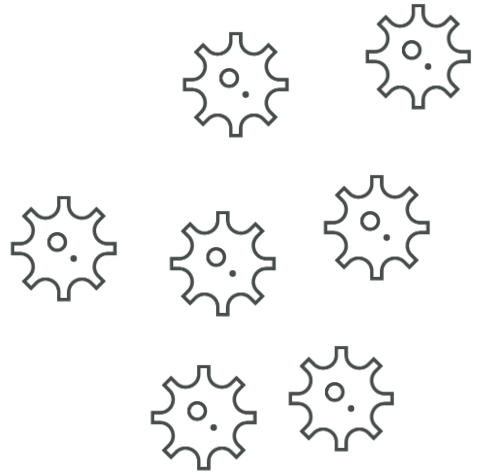
Grenzen der Versicherbarkeit bei Cyberrisiken?

Emerging Risks sind eine Herausforderung für die Grenzen der Versicherbarkeit.

Einige Kriterien stellen die Branche immer noch vor Herausforderungen.

Nur durch Begrenzungen der Limite, können Kriterien wie Korrelationen und die Zufälligkeit derzeit eingegrenzt werden.

- Legalität
- Eindeutigkeit des Schadenereignisses
- Zufälligkeit des Schadenereignis
- Verlässlichkeit der Wahrscheinlichkeiten
- Korrelation von Schadenereignissen
- Haftungsgrenzen / Schadenlimit



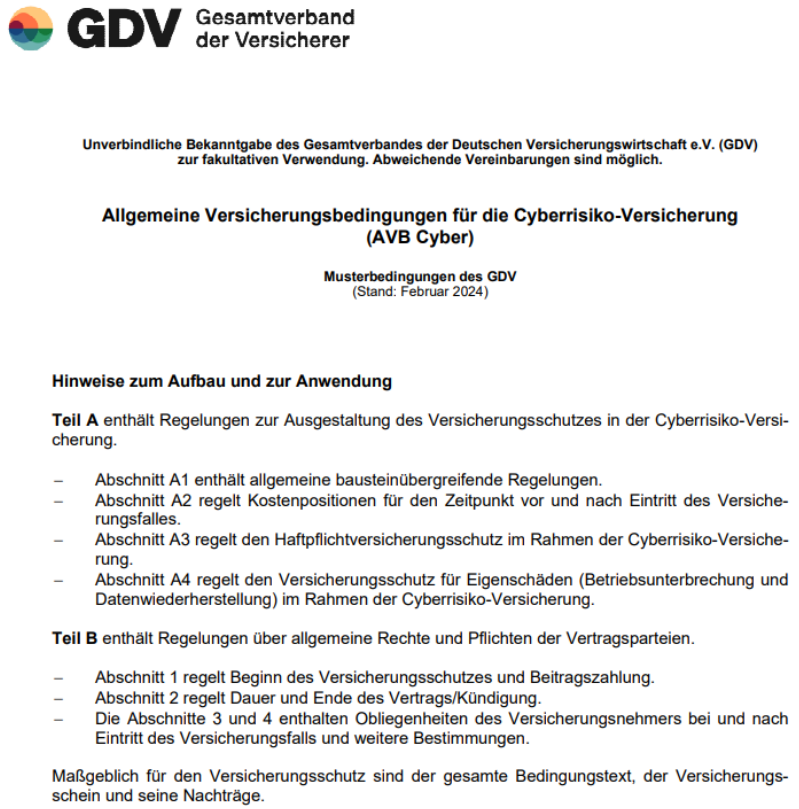
Cyber-Risk & Cyber-Governance – von neuen Geschäftsfeldern…
Überblick Emerging Risk Cyberrisiko

Grenzen der Versicherbarkeit bei Cyberrisiken?

Fakt ist aber auch, dass derzeit zahlreiche Versicherer eine Cyberversicherung anbieten.

Zuletzt aktualisierte dazu der **GDV** seine Musterbedingugen für die Cyberrisiko-Versicherung (Stand: Februar 2024)

- Legalität
- Eindeutigkeit des Schadenereignisses
- Zufälligkeit des Schadenereignis
- Verlässlichkeit der Wahrscheinlichkeiten
- Korrelation von Schadenereignissen
- Haftungsgrenzen / Schadenlimit



GDV Gesamtverband der Versicherer

Unverbindliche Bekanntgabe des Gesamtverbandes der Deutschen Versicherungswirtschaft e.V. (GDV) zur fakultativen Verwendung. Abweichende Vereinbarungen sind möglich.

Allgemeine Versicherungsbedingungen für die Cyberrisiko-Versicherung (AVB Cyber)

Musterbedingungen des GDV
(Stand: Februar 2024)

Hinweise zum Aufbau und zur Anwendung

Teil A enthält Regelungen zur Ausgestaltung des Versicherungsschutzes in der Cyberrisiko-Versicherung.

- Abschnitt A1 enthält allgemeine bausteinübergreifende Regelungen.
- Abschnitt A2 regelt Kostenpositionen für den Zeitpunkt vor und nach Eintritt des Versicherungsfalles.
- Abschnitt A3 regelt den Haftpflichtversicherungsschutz im Rahmen der Cyberrisiko-Versicherung.
- Abschnitt A4 regelt den Versicherungsschutz für Eigenschäden (Betriebsunterbrechung und Datenwiederherstellung) im Rahmen der Cyberrisiko-Versicherung.

Teil B enthält Regelungen über allgemeine Rechte und Pflichten der Vertragsparteien.

- Abschnitt 1 regelt Beginn des Versicherungsschutzes und Beitragszahlung.
- Abschnitt 2 regelt Dauer und Ende des Vertrags/Kündigung.
- Die Abschnitte 3 und 4 enthalten Obliegenheiten des Versicherungsnehmers bei und nach Eintritt des Versicherungsfalls und weitere Bestimmungen.

Maßgeblich für den Versicherungsschutz sind der gesamte Bedingungstext, der Versicherungsschein und seine Nachträge.

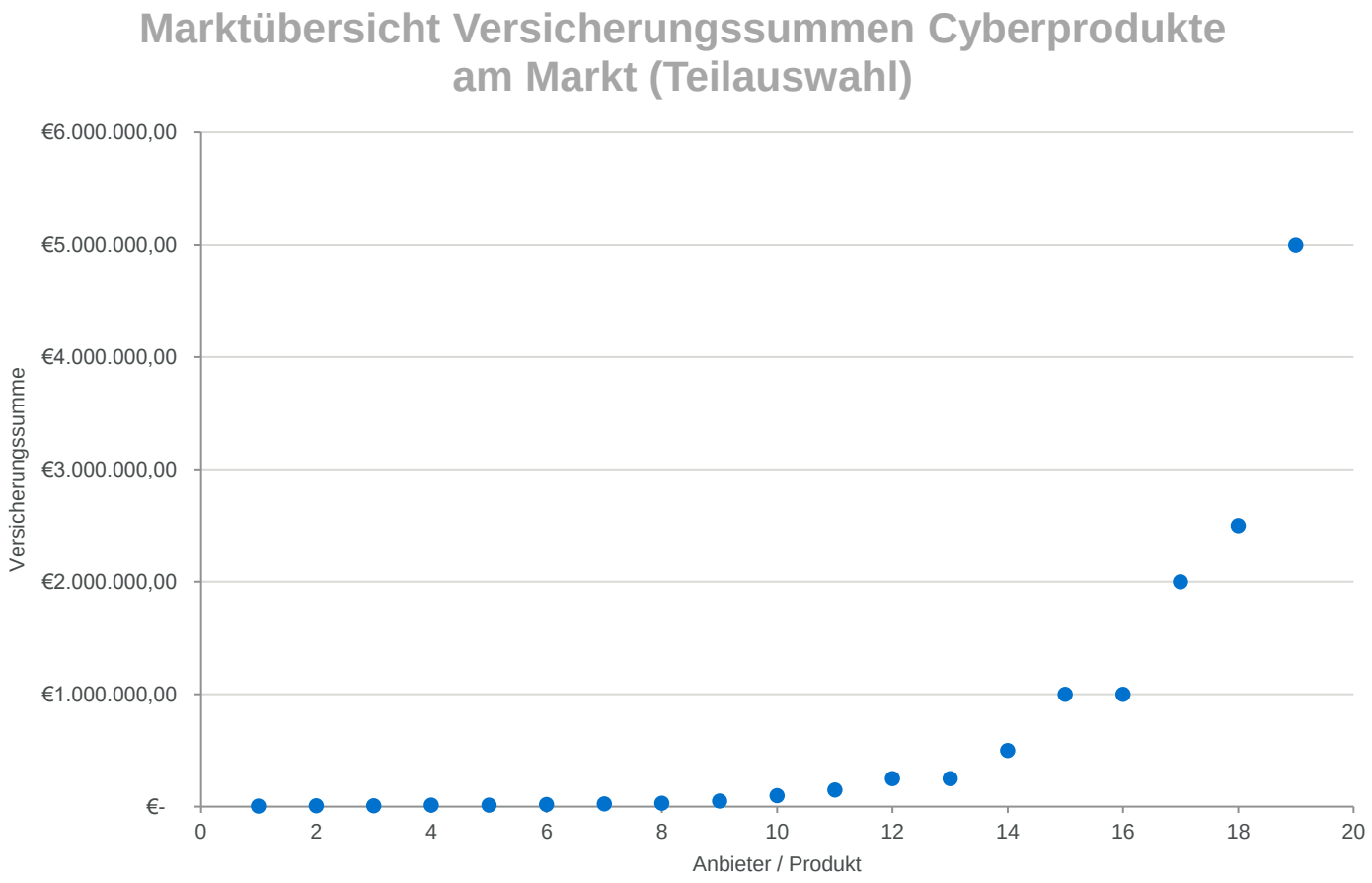
Quelle: (08.07.2024 / 9:00) https://www.gdv.de/resource/blob/6100/a0fed56c4947751cdc20b5206c171d98/01-allgemeine-versicherungsbedingungen-fuer-die-cyberrisiko-versicherung-avb-cyber--data.pdf

forvis mazars

Cyber-Risk & Cyber-Governance – von neuen Geschäftsfeldern…

Überblick Emerging Risk Cyberrisiko

Cyberversicherungen am Markt



Die Marktdurchdringung bzw. Produktportfoliodurchdringung der Cyberversicherungen ist bereits entwickelt.

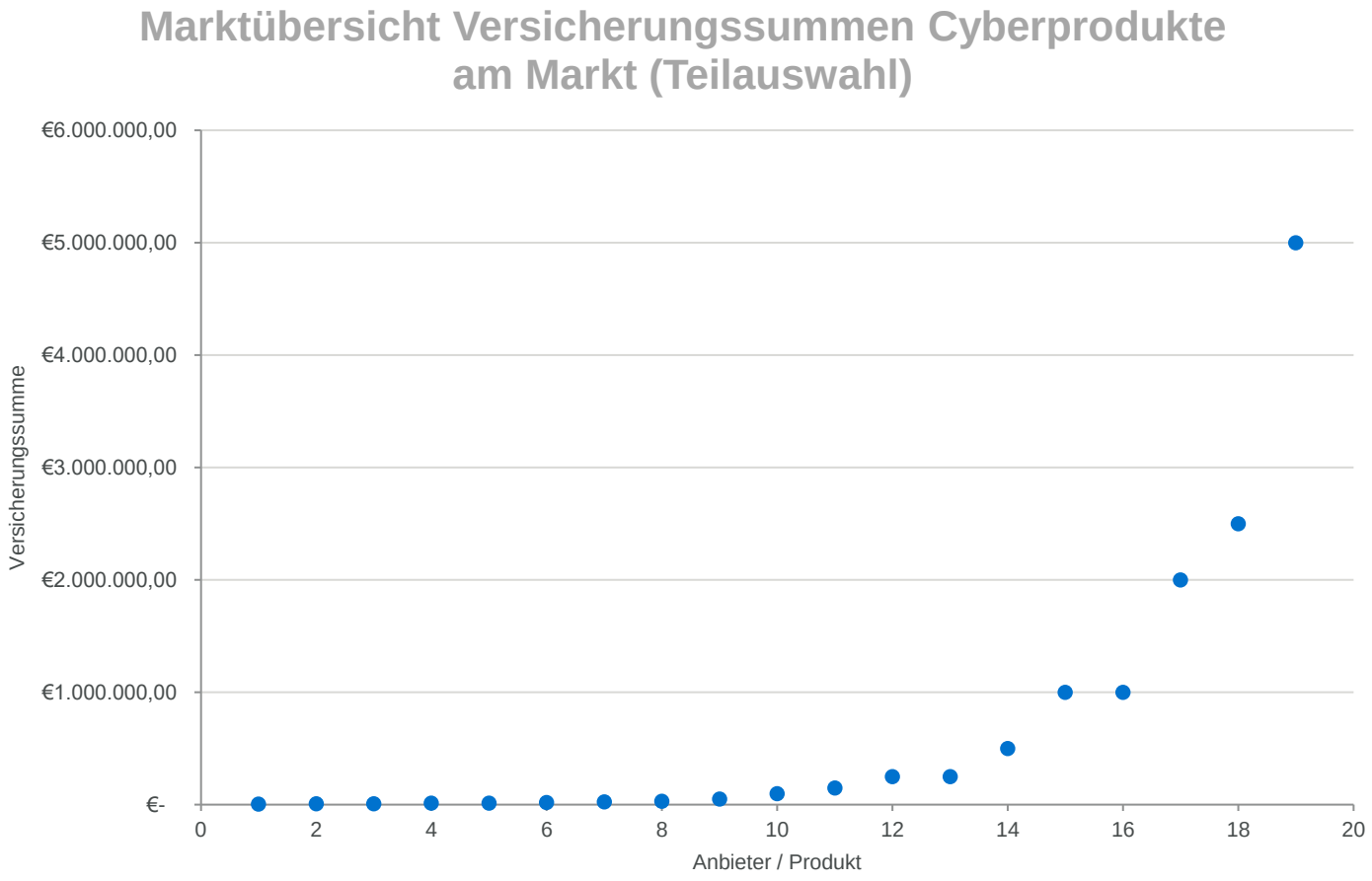
Sowohl Privat- wie auch Firmenkunden können Versicherungsschutz erwerben, ohne auf reine Spezialisten angewiesen zu sein.

Limite ergeben sich in der Teilauswahl insbesondere im Bereich der Versicherungssumme. Versicherungssummen lagen insbesondere bei Spezialanbietern höher.

Cyber-Risk & Cyber-Governance – von neuen Geschäftsfeldern…

Überblick Emerging Risk Cyberrisiko

Cyberversicherungen am Markt



In 2 Minuten zu Ihrem Angebot

	BESTSELLER		
	S GRUNDSCHUTZ	M GUT VERSICHERT	L TOP-SCHUTZ
Versicherungssumme	✓ 5 Mio. €	✓ 30 Mio. €	✓ 60 Mio. €
Tägliches Kündigungsrecht	✓	✓	✓
Schäden durch Gefälligkeiten	×	✓	✓
Schäden an geliehenen Sachen	×	×	✓
Schutz bei Forderungsausfall	×	✓ wählbar	✓

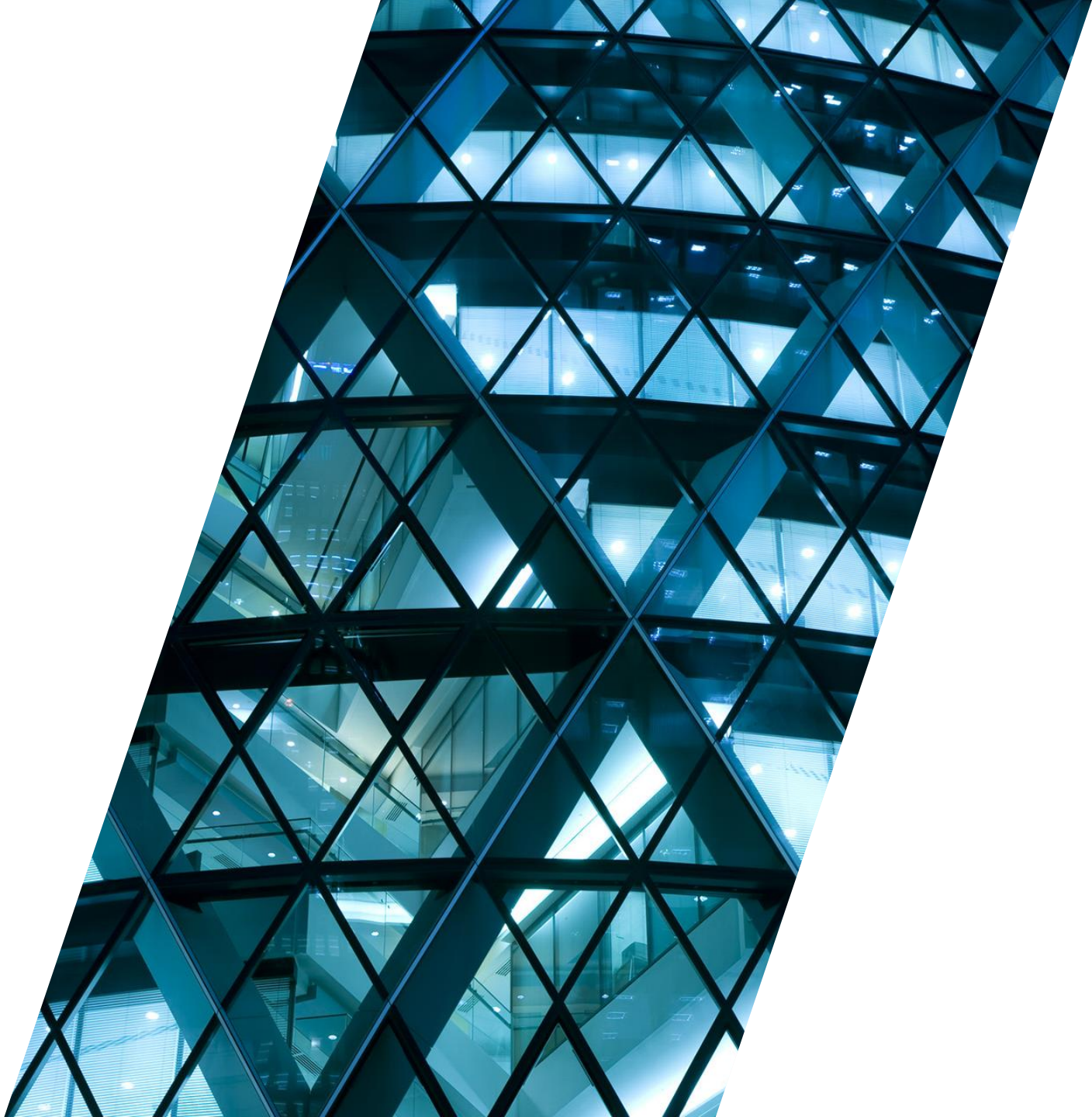
Cyber-Risk & Cyber-Governance – von neuen Geschäftsfeldern…

Worum es bisher ging….

02

Regulatorische Aspekte Cyberrisiko Versicherungsbranche

1. Überblick über Regulierung und Governance
2. DORA-Verordnung / FinmadiG



Cyber-Risk & Cyber-Governance –… und regulatorischen Herausforderungen
Regulatorische Aspekte Cyberrisiko Versicherungsbranche

VAG, HGB, BerVersV …. von Cyber keine Spur?

Weder im VAG, noch im HGB oder in der BerVersV ist der Begriff „Cyber“ zu finden.

Auch die Schlagworte „Informationstechnologie“ oder „Kommunikationstechnologie“ findet man nicht eindeutig.

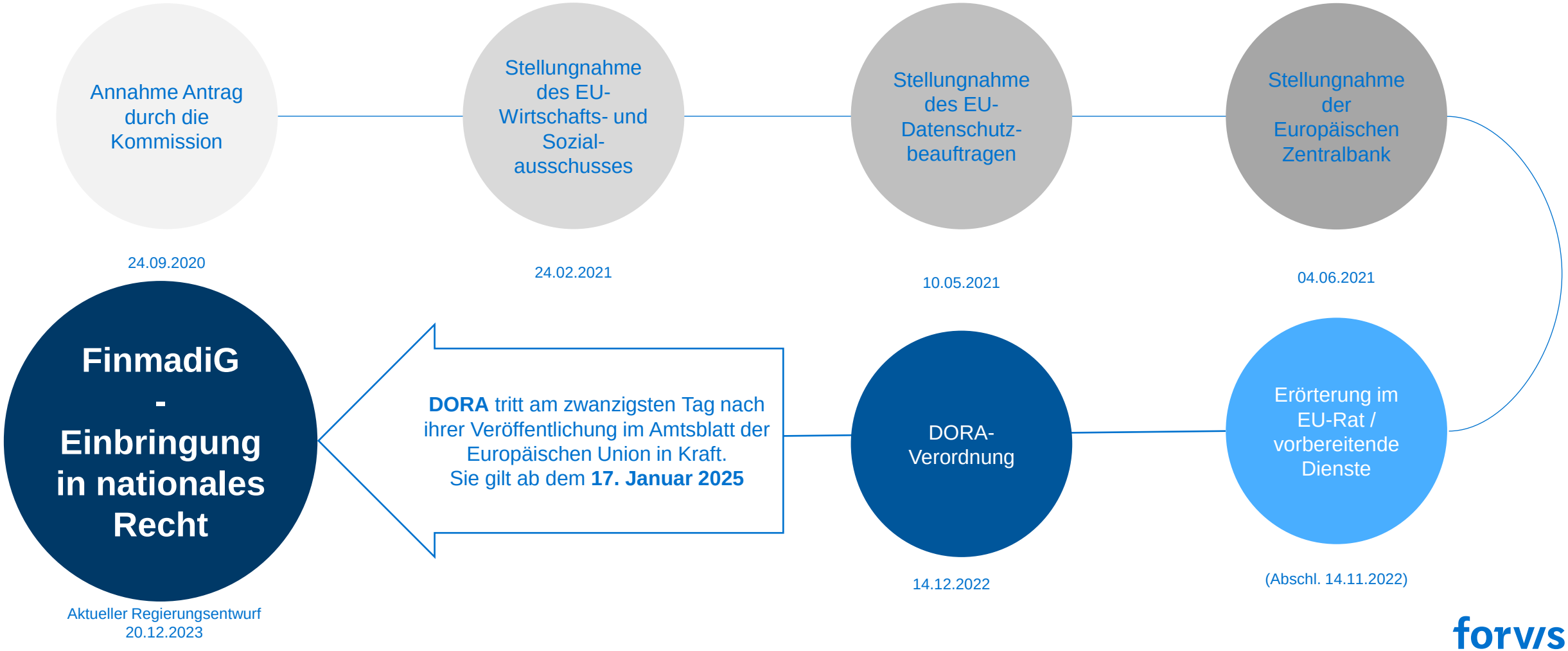
Cyber-Risk & Cyber-Governance –… und regulatorischen Herausforderungen
Regulatorische Aspekte Cyberrisiko Versicherungsbranche

DORA (Verordnung (EU) 2022/2554) – Digital Operational Resilience Act

Mit **DORA (Verordnung (EU) 2022/2554), dem (Digital Operational Resilience Act),** hat die EU eine für den Finanzsektor maßgebliche Regulierung für die Themen **Cybersicherheit, IKT-Risiken** und **digitale operationelle Resilienz** geschaffen.

Cyber-Risk & Cyber-Governance –… und regulatorischen Herausforderungen
Regulatorische Aspekte Cyberrisiko Versicherungsbranche

DORA → Finanzmarktdigitalisierungsgesetz (FinmadiG)



Cyber-Risk & Cyber-Governance –… und regulatorischen Herausforderungen
Regulatorische Aspekte Cyberrisiko Versicherungsbranche

Finanzmarktdigitalisierungsgesetz (FinmadiG)

Bundesministerium der Finanzen

Gesetzesentwurf

der Bundesregierung

Entwurf eines Gesetzes über die Digitalisierung des Finanzmarktes

(Finanzmarktdigitalisierungsgesetz – FinmadiG)

E.2 Erfüllungsaufwand Wirtschaft

Für die Wirtschaft ergibt sich eine Änderung des jährlichen Erfüllungsaufwands in Höhe von rund +605 000 Euro. Davon entfallen rund 292 000 Euro auf Bürokratiekosten aus Informationspflichten.

Der Erfüllungsaufwand für die Wirtschaft resultiert im Wesentlichen aus der 1 zu 1 Durchführung der Verordnungen (EU) 2023/1113, (EU) 2023/1114, (EU) 2022/2554 bzw. einer 1 zu 1 Umsetzung der Richtlinie (EU) 2022/2556. Insoweit wurde der Erfüllungsaufwand bereits von der Europäischen Kommission im Rahmen ihrer Folgenabschätzung für die gesamte Europäische Union beziffert. Die von der Bundesregierung beschlossene „one in one out"-Regel findet insoweit keine Anwendung. Im Übrigen ergibt sich ein „In" in Höhe von 332 000 Euro im Sinne der „one in one out"-Regelung der Bundesregierung.

Quelle: https://www.bundesfinanzministerium.de/Content/DE/Gesetzestexte/Gesetze_Gesetzesvorhaben/Abteilungen/Abteilung_VII/20_Legislaturperiode/2023-12-20-FinmadiG/0-Gesetz.html

Cyber-Risk & Cyber-Governance –… und regulatorischen Herausforderungen
Regulatorische Aspekte Cyberrisiko Versicherungsbranche

Finanzmarktdigitalisierungsgesetz (FinmadiG)

Inhaltsübersicht

Cyber-Risk & Cyber-Governance –… und regulatorischen Herausforderungen
Regulatorische Aspekte Cyberrisiko Versicherungsbranche

Finanzmarktdigitalisierungsgesetz (FinmadiG)

Inhaltsübersicht

Artikel 7

Änderung des Handelsgesetzbuches

§ 334 Absatz 4 Nummer 1 des Handelsgesetzbuches in der im Bundesgesetzblatt Teil III, Gliederungsnummer 4100-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 1 des Gesetzes vom 19. Juni 2023 (BGBl. 2023 I Nr. 154) geändert worden ist, wird wie folgt gefasst:

„1. die Bundesanstalt für Finanzdienstleistungsaufsicht in den Fällen des Absatzes 1 bei Kapitalgesellschaften, die kapitalmarktorientiert im Sinne des § 264d oder Institute nach § 37 Absatz 1 Satz 1 des Kryptomärkteaufsichtsgesetzes sind,“.

Cyber-Risk & Cyber-Governance –… und regulatorischen Herausforderungen
Regulatorische Aspekte Cyberrisiko Versicherungsbranche

Finanzmarktdigitalisierungsgesetz (FinmadiG)

Inhaltsübersicht

Artikel 1	Gesetz zur Aufsicht über Märkte für Kryptowerte (Kryptomärkteaufsichtsgesetz – KMAG)
Artikel 2	Änderung des Kryptomärkteaufsichtsgesetzes
Artikel 3	Änderung des Kreditwesengesetzes
Artikel 4	Änderung des Wertpapierhandelsgesetzes
Artikel 5	Änderung des Wertpapierinstitutsgesetzes
Artikel 6	Änderung des Kapitalanlagegesetzbuches
Artikel 7	Änderung des Handelsgesetzbuches
Artikel 8	Änderung des Geldwäschegesetzes
Artikel 9	Änderung der Gewerbeordnung
Artikel 10	Änderung des Börsengesetzes
Artikel 11	Änderung des Versicherungsaufsichtsgesetzes
Artikel 12	Änderung des Zahlungsdiensteaufsichtsgesetzes
Artikel 13	Änderung des Sanierungs- und Abwicklungsgesetzes
Artikel 14	Änderung des Gerichtsverfassungsgesetzes

I. §35 – Pflichten des Abschlussprüfers

II. §293 – Aufsicht – Versicherungs-Holdinggesellschaften und gemischte Finanzholding-Gesellschaften

III. §295 – Zuständige Behörde in Bezug auf EU-Verordnungen (Teil 6 – Aufsicht)
IV. §308d (NEU) – Befugnisse der Aufsicht
V. §310 – Nebenbestimmungen; Ausschluss der aufschiebenden Wirkung
VI. §319a – Bekanntmachung von Maßnahmen und Sanktionen wegen Verstößen gegen Verordnungen
VII. §332 – Bußgeldvorschriften

Cyber-Risk & Cyber-Governance –… und regulatorischen Herausforderungen
Fokus auf Digital Operational Resilience Act (DORA)

Erläuterung der Norm

Offizieller Text

Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011 - **Anzuwenden ab: 17. Januar 2025**

Auslöser systemisches Risiko

- Zunahme der Cyberbedrohungen (Häufigkeit)
- Digitalisierung des Finanzsystems (Exposition)
- Heterogenität des regulatorischen Umfelds auf europäischer Ebene (Anfälligkeit)
- Wachsende Bedeutung von IKT-Anbietern

Folge der jüngsten gesetzlichen Entwicklungen

- ENISA – NIS Directive Finanzsystems (Exposition)
- Internationalen Empfehlungen, an denen die ECB teilnahm (G7 Cyber Expert Group, CPMI-IOSCO Guidance on cyber)
- Nationale Aufsichtsbehörden haben Befugnisse, die Einhaltung der Verordnung durchzusetzen

Anwendungsbereiche

Finanzunternehmen und IKT-Dienstleistern (Informations- und Kommunikationstechnologie), darunter :
- Banken
- Versicherungsgesellschaften
- Zahlungsdienstleister
- Anbieter von Krypto-Assets und weitere

Der Anwendungsbereich umfasst alle relevanten Akteure, die Teil des Finanzsystems sind, und schließt auch kritische Drittanbieter ein. (Weiter unten ausführlicher).

Für den EU-Raum:
~22.000 Business Units und 15.000 Einrichtungen

Cyber-Risk & Cyber-Governance –… und regulatorischen Herausforderungen
Fokus auf Digital Operational Resilience Act (DORA)

Finanzmarktdigitalisierungsgesetz (FinmadiG)

DORA Verordnung 2022/2554

Wer ist betoffen?

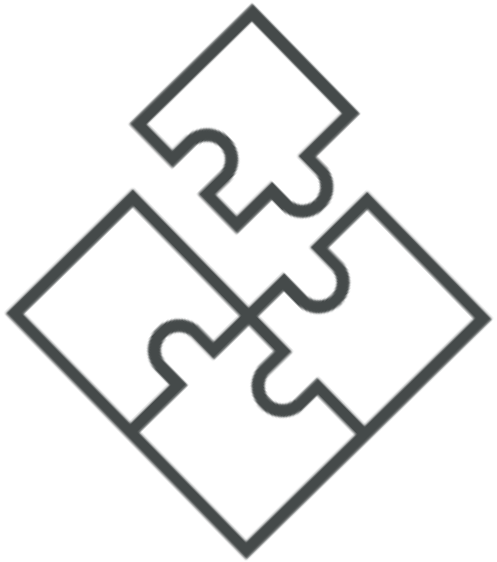
Im Geltungsbereich:	Ausnahmen:
Versicherungsunternehmen	Versicherungsunternehmen, welche unter Artikel 4 RiLi 20090/138/EG fallen
Rückversicherungsunternehmen	Rückversicherungsunternehmen, welche unter Artikel 4 RiLi 2009/138/EG fallen
Versicherungsvermittler	EbAVs mit weniger als 15 Versorgungsanwärter
Einrichtungen der betrieblichen Altersversorgung	

Cyber-Risk & Cyber-Governance –… und regulatorischen Herausforderungen
Fokus auf Digital Operational Resilience Act (DORA)

Finanzmarktdigitalisierungsgesetz (FinmadiG)

DORA Verordnung 2022/2554

Eckpunkte / Gegenstand



- **Risikomanagement** im Bereich IKT
- **Meldungen schwerwiegender IKT-bezogener Vorfälle**
- Meldung schwerwiegender zahlungsbezogener Betriebs- oder Sicherheitsvorfälle
- **Test der digitalen operationalen Resilienz**
- Austausch / Informationen / Erkenntnisse bzgl. Cyberbedrohungen
- Maßnahmen für das solide Management des **IKT-Drittparteienrisikos**

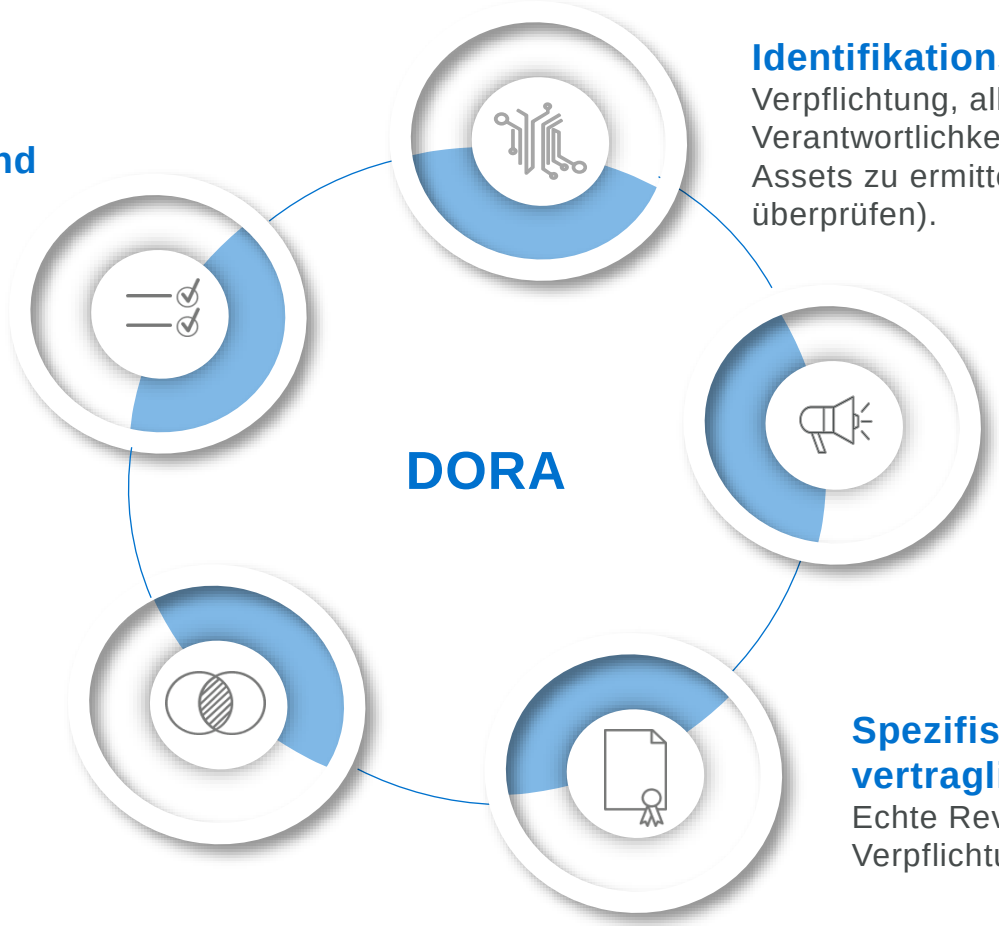
- Anforderungen bzgl. vertragl. Vereinbarungen zwischen IKT-Drittdienstleistern und Finanzunternehmen
- Vorschriften Überwachungsrahmen für kritische IKT-Drittdienstleister bei der Erbringung von Dienstleistungen
- Vorschriften bzgl. Zusammenarbeit zuständiger Behörden und Durchsetzung der DORA-Sachverhalte

Cyber-Risk & Cyber-Governance –… und regulatorischen Herausforderungen
Fokus auf Digital Operational Resilience Act (DORA)

DORA-Konzept im Überblick

Verschärfte Pflichten für kritische und wichtige Funktionen
- Definition
- Grundsatz der Verhältnismäßigkeit.
- Verstärkte technische Schutzmaßnahmen
- Interne und externe Resilienztests (Tests und Überprüfungen): Penetrationstests, Stresstests und Szenarioanalysen

Verwaltung von Drittanbietern
- Für kritische Drittanbieter von IKT-Dienstleistungen
- Verträge müssen klare Bestimmungen enthalten, um die Einhaltung von DORA zu gewährleisten
- IKT ist regelmäßig durch Schwachstellentests zu prüfen



Identifikationspflicht
Verpflichtung, alle IKT-relevanten Verantwortlichkeiten, Verträge, Rollen, Systeme und Assets zu ermitteln und zu klassifizieren (jährlich zu überprüfen).

Meldepflicht bei größeren Sicherheitsvorfällen
- Ermöglicht eine schnelle Reaktion auf Vorfälle und eine koordinierte Reaktion auf Bedrohungen.
- Standardisiertes Verfahren zur Meldung und Nachverfolgung solcher Vorfälle

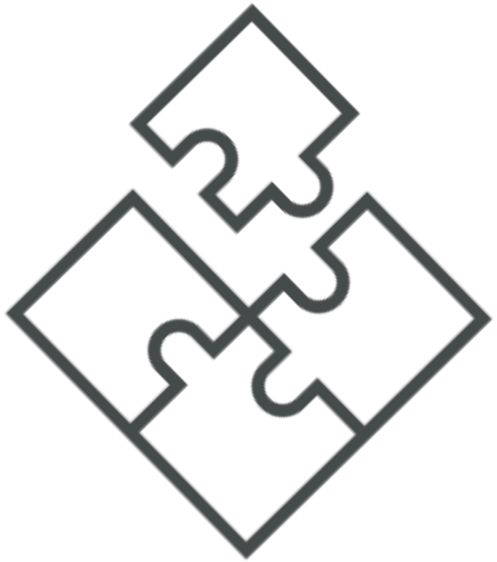
Spezifischer und sehr detaillierter vertraglicher Rahmen
Echte Revolution bei den Juristen, um alle Verpflichtungen zu erfassen

Cyber-Risk & Cyber-Governance –… und regulatorischen Herausforderungen
Fokus auf die Digital Operational Resilience Act (DORA) Richtlinie

Finanzmarktdigitalisierungsgesetz (FinmadiG)

DORA Verordnung 2022/2554

Eckpunkte / Gegenstand



Risikomanagement
im Bereich IKT

Meldungen schwerwiegender IKT-bezogener Vorfälle

Meldung schwerwiegender zahlungsbezogener Betriebs- oder Sicherheitsvorfälle

Test der digitalen operationalen Resilienz

Austausch / Informationen / Erkenntnisse bzgl. Cyberbedrohungen

Maßnahmen für das solide Management des **IKT-Drittparteienrisikos**

Anforderungen bzgl. vertragl. Vereinbarungen zwischen IKT-Drittdienstleistern und Finanzunternehmen

Vorschriften Überwachungsrahmen für kritische IKT-Drittdienstleister bei der Erbringung von Dienstleistungen

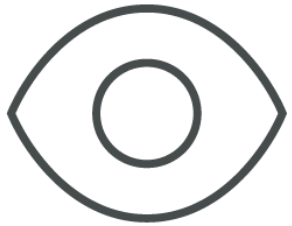
Vorschriften bzgl. Zusammenarbeit zuständiger Behörden und Durchsetzung der DORA-Sachverhalte

Cyber-Risk & Cyber-Governance –… und regulatorischen Herausforderungen
Fokus auf Digital Operational Resilience Act (DORA)

Finanzmarktdigitalisierungsgesetz (FinmadiG)

DORA Verordnung 2022/2554

Governance im Bereich IKT



Governance:

- Zuweisung klarer Rollen und Zuständigkeiten für alle IKT-bezogenen Funktionen
- Kontinuierliches Engagement bei der Überwachung des IKT-Risikomanagements und der Genehmigungs- und Kontrollverfahren
- Angemessene Zuweisung von IKT-Investitionen und –Schulungen

Risikomanagement(-rahmen):

- Das Risikomanagement orientiert sich an branchenspezifischen Leitlinien und Normen und umfasst insbesondere
  - Die Minimierung von IKT-Risiken und kontinuierliche Ermittlung der Ursachen als Aufgabe der Unternehmen
  - Ergreifung von Schutz- und Präventionsmaßnahmen
  - Aufdeckung ungewöhnlicher Aktivitäten
  - Entwicklung einer umfassenden Strategie für die Fortführung des Betriebes
  - Erstellung von Notfall- und Wiederherstellungsplänen

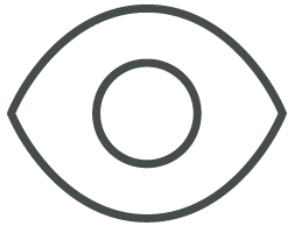
Quellen: (Vortrag BaFin im Rahmen der IT-Aufsicht bei Versicherungen und Pensionsfonds“, pdf (europa.eu))

Cyber-Risk & Cyber-Governance –… und regulatorischen Herausforderungen
Fokus auf Digital Operational Resilience Act (DORA)

Finanzmarktdigitalisierungsgesetz (FinmadiG)

DORA Verordnung 2022/2554

Governance im Bereich IKT



Governance:

Das Leitungsorgan

- weist **angemessene Budgetmittel zu** und überprüft diese regelmäßig, um den Anforderungen des Finanzunternehmens an die digitale operationale Resilienz in Bezug auf alle Arten von Ressourcen gerecht zu werden,
- **einschließlich einschlägiger Programme zur Sensibilisierung** für IKT-Sicherheit und Schulungen zur digitalen operationalen Resilienz nach Artikel 13 Absatz 6 sowie IKT-Kompetenzen
- **für alle Mitarbeiter**

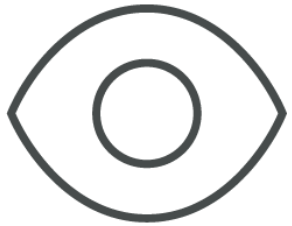
Cyber-Risk & Cyber-Governance –… und regulatorischen Herausforderungen
Fokus auf Digital Operational Resilience Act (DORA)

Finanzmarktdigitalisierungsgesetz (FinmadiG)

DORA Verordnung 2022/2554

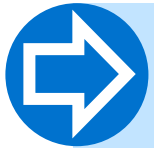
Governance / Risikomanagementrahmen (organisatorisch):

Governance im Bereich IKT



Finanzunternehmen, bei denen es sich nicht um Kleinstunternehmen handelt,

- übertragen **die Zuständigkeit für das Management** und die Überwachung des IKT-Risikos an eine Kontrollfunktion
- und stellen ein angemessenes Maß an Unabhängigkeit dieser Kontrollfunktion sicher, um Interessenkonflikte zu vermeiden.
- **angemessene Trennung und Unabhängigkeit von IKT-Risikomanagementfunktionen,** Kontrollfunktionen und internen Revisionsfunktionen gemäß dem Modell der **drei Verteidigungslinien** oder einem internen Modell für Risikomanagement und Kontrolle.



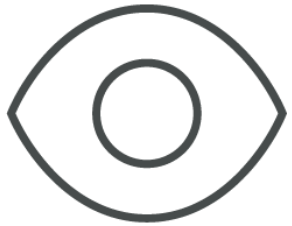
Analogie zu Solvency II

Cyber-Risk & Cyber-Governance –… und regulatorischen Herausforderungen
Fokus auf Digital Operational Resilience Act (DORA)

Finanzmarktdigitalisierungsgesetz (FinmadiG)

DORA Verordnung 2022/2554

Governance im Bereich IKT

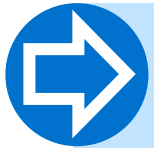


Governance / Risikomanagementrahmen (organisatorisch):

Der IKT-Risikomanagementrahmen wird…

- mindestens einmal jährlich
- regelmäßig (bei Kleinstunternehmen)
- bei Auftreten schwerwiegender IKT-bezogener Vorfälle
- nach aufsichtsrechtlichen Anweisungen oder Feststellungen

…dokumentiert und überprüft

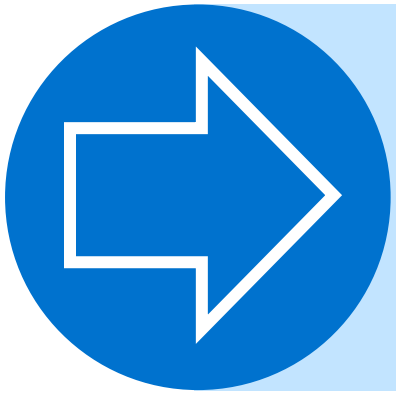


Analogie zu Solvency II

Cyber-Risk & Cyber-Governance –… und regulatorischen Herausforderungen
Fokus auf Digital Operational Resilience Act (DORA)

Rahmen für das Risikomanagement und Governance

Die Verordnung verpflichtet Finanzunternehmen, robuste Risikomanagementstrategien einzuführen und einen umfassenden Rahmen für das Management von IKT-Risiken zu schaffen. Dazu gehören klare Verantwortlichkeiten und Prozesse zur Identifizierung, Bewertung und Abschwächung von IKT-Risiken sowie Maßnahmen zur Erkennung, Vermeidung, Reaktion und Wiederherstellung.



Analogie zu Solvency II / VAIT (VA) / R 10/2018 (VA)

Kann Solvency II als schematisches (aktuarielles) Vorbild dienen?

Der DORA-Prozess verstärkt die bereits unter Solvency II eingeführten Maßnahmen

- Übergang von einem Soft Law mit EIOPA-Leitlinien zu „Hard Law“
- Kontinuität im Risikomanagement, da Risiko bereits erfasst ist
- Der DORA-Scope von IKT-Anbietern ist breiter als der von Solvabilität II.
- Alle vertraglichen Vereinbarungen müssen in einem Vertragsregister erfasst und registriert werden.
- Die Idee von Solvency II wird mit der Ernennung einer Funktion ähnlich einer Schlüsselfunktion wieder aufgegriffen. Diese berichtet an den Verwaltungsrat, der die Mittel und Vorkehrungen in einem Bericht überprüft und die Pläne zur operationellen Widerstandsfähigkeit bestätigt.
- Begriff der digitalen operativen Resilienzstrategie
- Mehrere potenzielle Eigentümer: Nutzer, CIO, Compliance, DPO DSGVO, Rechtsabteilung, Risikomanagement.

Cyber-Risk & Cyber-Governance –… und regulatorischen Herausforderungen
Fokus auf Digital Operational Resilience Act (DORA)

Rahmen für das Risikomanagement und Governance

Rundschreiben (VA) 10/2018 (VA) (03.03.2022)
VAIT

BaFin
Bundesanstalt für Finanzdienstleistungsaufsicht

Inhalt

Artikel	Inhalt
1	Gegenstand
2	Geltungsbereich
3	Begriffsbestimmungen
4	Grundsatz der Verhältnismäßigkeit
5	Governance und Organisation
6	IKT-Risikomanagement
7	IKT-Systeme, -Protokolle und -Tools
8	Identifizierung
9	Schutz und Prävention
10	Erkennung
11	Reaktion und Wiederherstellung
12	Wiedergewinnung und Wiederherstellung
13	Lernprozesse und Weiterentwicklung
14	Kommunikation
15	Harmonisierung (Tools, Assets, Prozesse, …)
16	Vereinfachter IKT-Risikomanagementrahmen
17	Behandlung IKT-bezogender Vorfälle
18	Klassifizierung IKT-bezogene Vorfälle / Cyberbedrohungen
19	Meldungen IKT-Vorfälle / freiwillige Meldungen Cyberbedrohungen
20	Harmonisierung von Inhalt, Vorlagen und Meldungen
21	Zentralisierung der Berichterstattung IKT-Vorfälle
22	Rückmeldung von Aufsichtsbehörden
23	Zahlungsbezogene Betriebs- und Sicherheitsvorfälle
24	Allg. Anforderungen Testen der digitalen op. Resilienz
25	Testen von IKT-Tools und - Systemen
26	Erweiterte Tests von IKT-Tools, -Systeme und -Prozesse
27	Anford. Tester bezgl. Durchführung von TLPT
28	IKT-Drittparteienrisiko (Allgemeine Prinzipien)
29	Bewertung IKT-Konzentrationsrisikos
30	Wesentliche Vertragsbestimmungen IKT-Drittdienstl.
31	Einstufung kritische IKT-Drittdienstl.
32	Strukturen und Überwachungsrahmen
33	Aufgaben Überwachungsbehörde
34	Op. Zusammenarbeit der Überwachungsbehörde
35	Befugnisse der Überwachungsbehörde
36	Befügnisse außerhalb der Union
37	Auskunftsersuchen
38	Allgemeine Untersuchungen
39	Inspektionen
40	Laufende Überwachung
41	Harmonisierung Überwachungstätigkeiten
42	Folgemaßnahmen zust. Behörden
43	Überwachungsgebühr
44	Internat. Zusammenarbeit
45	Austausch von Informationen und Erkenntnissen
46	Zusammenarbeit der Behörden
	… weitere

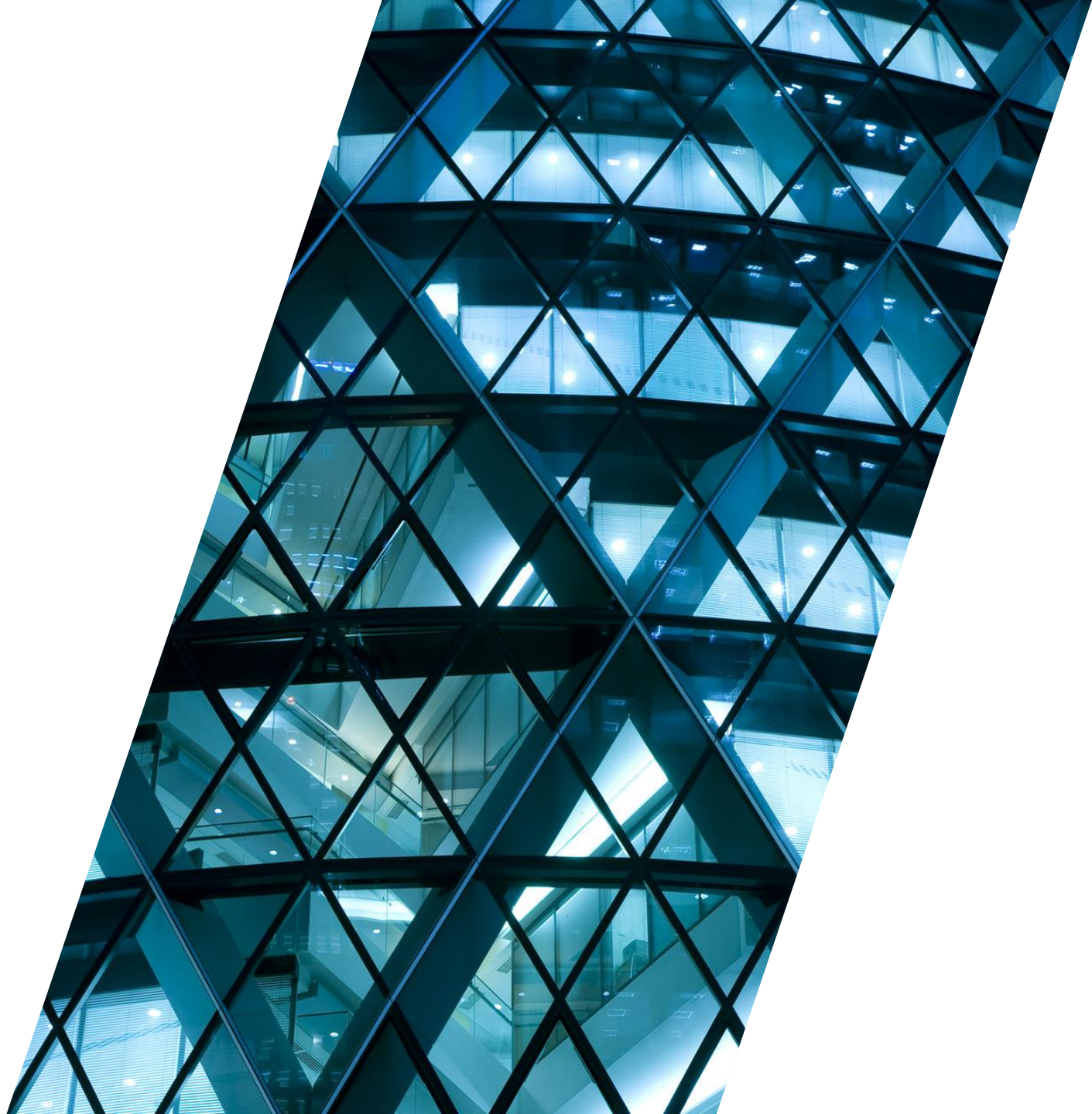
forvis mazars

Cyber-Risk & Cyber-Governance –… und regulatorischen Herausforderungen

Worum es bisher ging….

03

Herausforderungen für die Modellierung



Cyber-Risk & Cyber-Governance

Herausforderung in der Modellierung: Ausgewählte Quellen und Referenzen

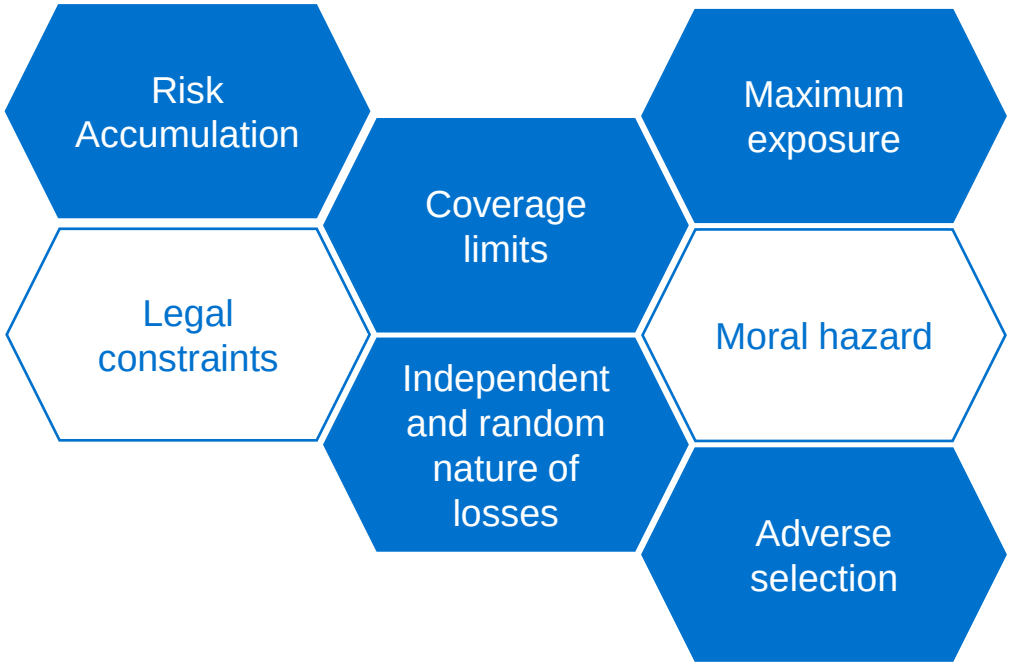
Referenzen (hauptsächlich für den Modellierungsteil)

- DAV: Ergebnisbericht des Ausschusses Schadenversicherung: Use Case der DAV AG Daten und Methoden zur Bewertung von Cyberrisiken.
- DAV: Ergebnisbericht des Ausschusses Schadenversicherung Cyberrisiken – Herausforderungen und Einfluss auf das Risikomanagement in Versicherungsunternehmen.
- DAV: Ergebnisbericht des Ausschusses Schadenversicherung Daten und Methoden zur Bewertung von Cyberrisiken.
- Modeling and Pricing Cyber Insurance – A Survey K. Awiszusa,d, T. Knispelb, I. Pennerc, G. Svindlanda, A. Voßa, and S. Webera, Modeling and Pricing Cyber Insurance – A Survey
- Identifikation von Lücken : Rapport 2023 IBM – cost of data breach
- Ansteckendes und systemisches Risiko : Systemic Cyber Risk: A Primer - Carnegie Endowment for International Peace
- Überprüfung der Versicherbarkeitskriterien : « Insurability of Cyber Risk : an emprical analysis » Insurability of Cyber Risk: An Empirical Analysis by Christian Biener, Martin Eling, Jan Hendrik Wirfs :: SSRN
- Starker Rückgriff auf Rückversicherungen : Les réassureurs avancent à l'aveugle sur le cyber (argusdelassurance.com)
- SIR-Modell : C. Hillairet et O. Lopez Cyber contagion: impact of the network structure on the losses of an insurance portfolio (chaire-pari.fr)
- SIR-Modell mit mehreren Gruppen : Travaux de C. Hillairet et O. Lopez Cyber contagion: impact of the network structure on the losses of an insurance portfolio (chaire-pari.fr) et Detra-Note-2021-4_Accumulation-scenarios-in-cyber-insurance..pdf (detralytics.com)
- Verschiedene Ansätze zur Modellierung : Modelling and Pricing Cyber Insurance – Idiosyncratic, Systematic, and Systemic Risk 2209.07415.pdf (arxiv.org)
- Entwicklungen in der Cybersicherheitsgesetzgebung in Europa, den USA und Asien : Mémoire de L'Institut des Actuaires, Guillaume Rigaud, Modèle d'accumulation du risque cyber
- Entwicklung Art der Angriffe Mariama Baldé. Optimisation de la structure de réassurance du risque Cyber.
- Mémoire de L'Institut des Actuaires, BEAUD DE BRIVE Gaëtan, Modélisation du risque cyber pour un portefeuille d'assurance français
- Webinar des „Institut des Actuaires“ über die DORA-Regelung

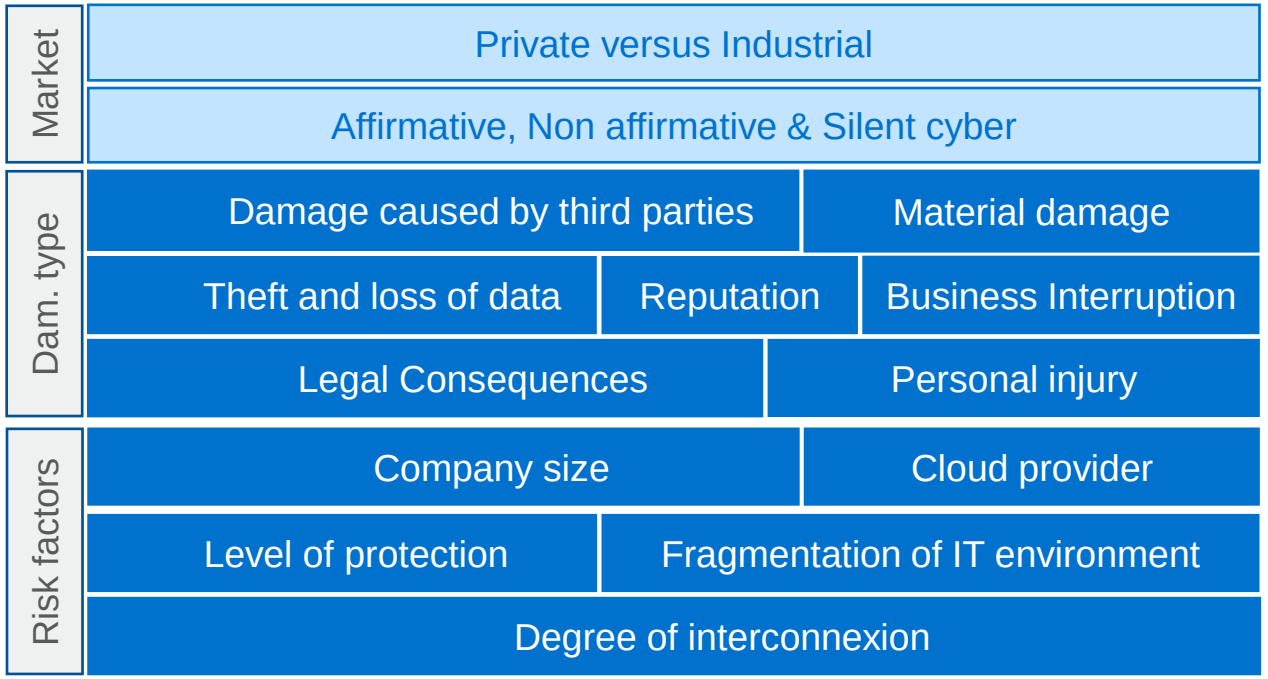
Cyber-Risk & Cyber-Governance –… und regulatorischen Herausforderungen **Herausforderung für die Modellierung**

Even with the increasing systemization of the risk, the cyber market is still facing insurability challenges.

Insurability



Systemization



Cyber-Risk & Cyber-Governance –… und regulatorischen Herausforderungen **Herausforderung für die Modellierung**

Despite insurance industry's advancement in recent years, cyber risk modeling remains a challenge.

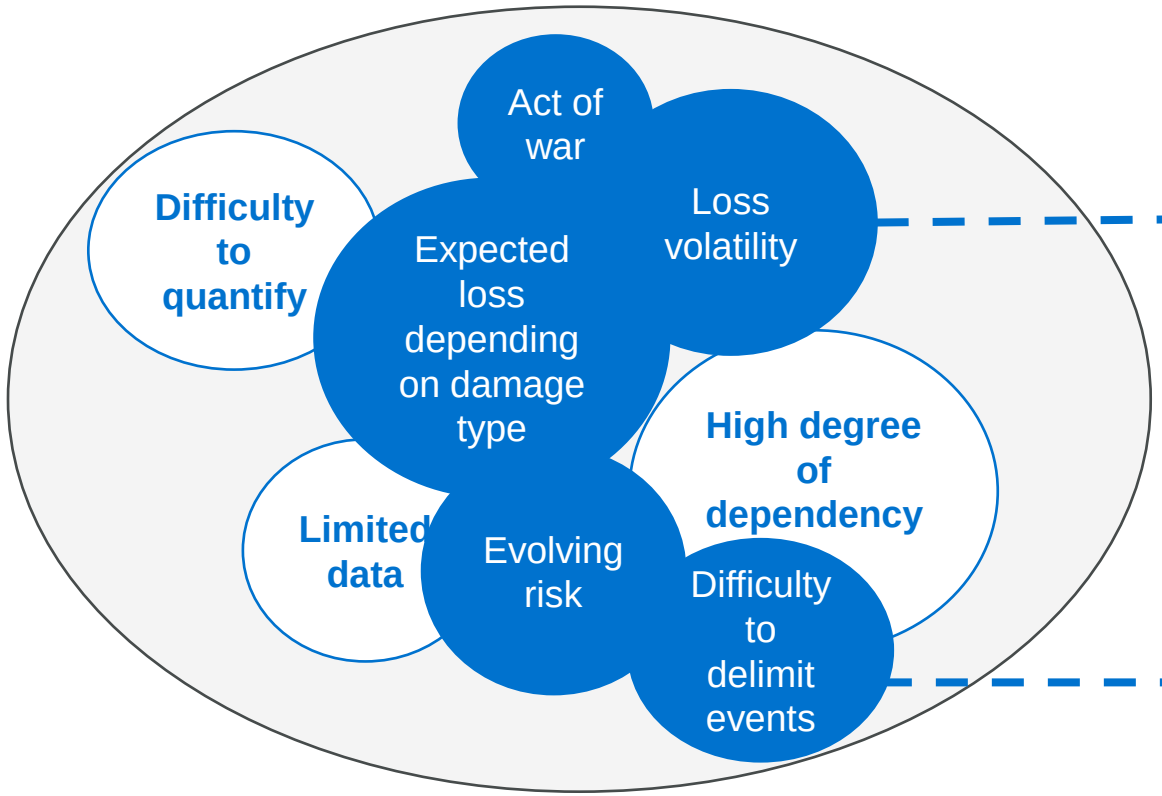


Exhibit 7: Cyber insurance loss ratio percentiles by year | insurers with WP greater than $5M

Standalone

Calendar Year	5th Pctl	25th Pctl	Median	75th Pctl	95th Pctl
2021	2%	25%	48%	73%	128%
2022	0%	12%	39%	53%	68%

Package

Calendar Year	5th Pctl	25th Pctl	Median	75th Pctl	95th Pctl
2021	7%	16%	32%	84%	354%
2022	3%	13%	31%	63%	178%

Total

Calendar Year	5th Pctl	25th Pctl	Median	75th Pctl	95th Pctl
2021	1%	20%	47%	78%	144%
2022	1%	15%	30%	54%	119%

U.S. Cyber Market Update, AON, September 2023.

Settlement of specific contracts
- Detection of the problem
- Implementation of repair action
- Identification of the source
- Protection/Prevention

Cyber-Risk & Cyber-Governance –… und regulatorischen Herausforderungen
Herausforderung für die Modellierung

Cyber modeling approaches are displayed as follow.

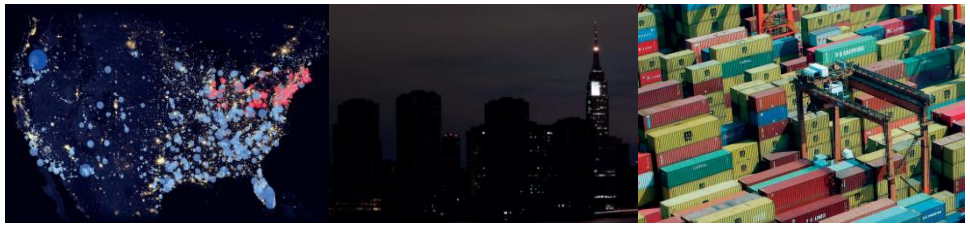
Cyber Modeling

- **Actuarial pricing**
- **Representation of cumulative risk**
- **Scenario analysis – to improve understanding of risks**

$$S = \sum_{i=1}^{N} Xi$$

- N: Random number of claims (frequency)
- Xi: Random Loss
- S: Expected Total Loss

Wikipedia illustration of Network topology



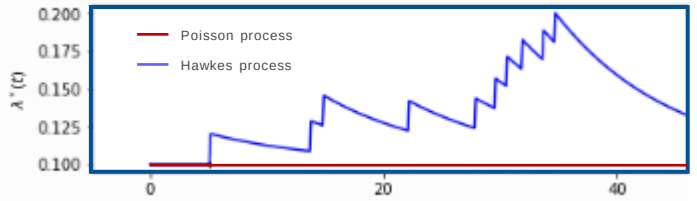
The insurance implications of a cyber attack on the US power
Lloyd's Emerging Risk Report, 2015

Cyber-Risk & Cyber-Governance –… und regulatorischen Herausforderungen
Herausforderung für die Modellierung

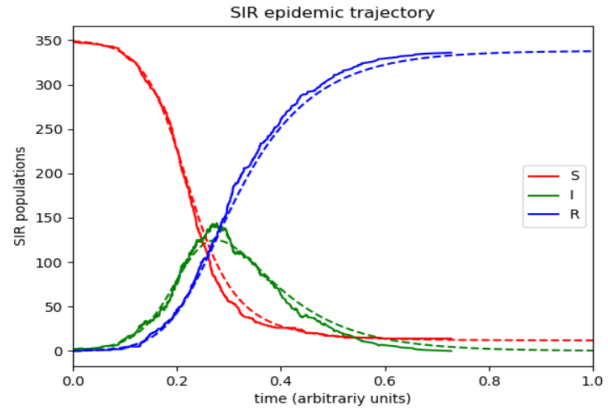
The most used frequency models are presented below.

The variety of risk factors remains the most challenging part of frequency modeling.

Model	Principles	Benefits	Drawbacks
Binomial law, Negative Binomial law, Poisson point process	Usual frequency law and counting process	Familiar and easy to use	Does not take self-correlations into account
Cox processes	Doubly stochastic Poisson process	Able to take self-correlations into account	More difficult to calibrate
Hawkes processes	Intensity as the sum of a Poisson process plus a self-excitation function	Able to take self-correlations into account	More difficult to calibrate
Epidemiological model (SIR)	Compartmental model The policyholders are assigned to compartments with labels (Susceptible, Infectious, or Recovered)	Better designed for Risk Management and scenario analysis Other validation approaches to consider	Not considered for pricing purpose Time-consuming assumption calibration



Illustrative example of the intensity of a Hawkes process, Python documentation on the package hawkeslib.readthedocs.io



Wikipedia illustration of the SIR model

Cyber-Risk & Cyber-Governance –… und regulatorischen Herausforderungen
Herausforderung für die Modellierung

Given the evolving nature of cyber risk, use of quickly adaptable models.

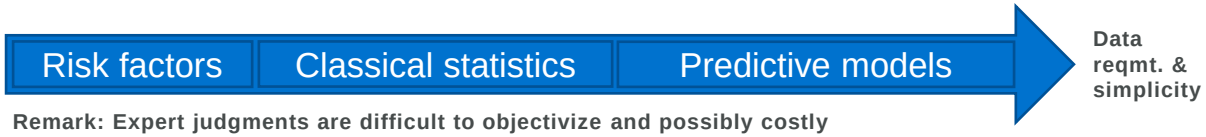
Classical statistic techniques can be used to model costs depending on the sub-risks measured:

- **Duration/Time** (Business Interruption): Exponential, Weibull, Gamma, Gompertz-Makeham.
- **Quantity** (number of stolen data lines):
  - Small & Large claims: Normal, Log-Normal, Gamma, Wald;
  - Extreme claims: Generalized Pareto, Fréchet, Weibull.

Cost modeling is based on **risk factors** (sector, sales, vulnerability).

A score is assigned to each risk factor. All scores are aggregated before being applied to an insured sum.

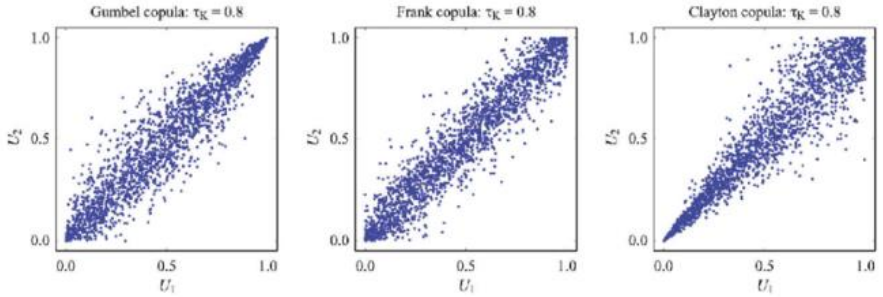
Predictive models such as GLM and Machine Learning algorithms are also possible but are still data-intensive. These models are more flexible and quicker to execute once calibrated/trained.



Remark: Expert judgments are difficult to objectivize and possibly costly

Once the **cost distributions are calibrated for each cyber sub-risk**, **correlations could be considered.** Since the initial analysis is based on calibrated marginal distributions, the use of **copula theory** could be appropriate for the determination of the final multivariate joint distribution.

Gaussian copula	Archimedean copulas (class)
$C_R(u) = \phi_R(\phi^{-1}(u_1),\ldots,\phi^{-1}(u_d))$	$C(u,\theta) = \psi(\psi^{-1}(u_1,\theta),\ldots,\psi^{-1}(u_{d,\theta}),\theta)$
ϕ^{-1} inverse cdf of a std normal. ϕ_R cdf of a multi. Normal dist.	ψ is at least d - 2 times continuously derivable, whose derivative of order d - 2 is convex decreasing, and such that $\psi(1)=0$
Easy to compute, only needs a correlation matrix.	Allow dependence in arbitrarily high dimensions, one single parameter, which governs the intensity of dependence



Cyber-Risk & Cyber-Governance –… und regulatorischen Herausforderungen

Herausforderung für die Modellierung

Scenario-based modeling as Risk management tool.

In the **scenario analysis**, first **we define an overall scenario**, then we **try to determine its impact on the portfolio**.

- "2015 emerging risk report", Lloyd's published a scenario on "The insurance implications of a cyber attack on the US power".
- Scenario of a cloud attack on one of the biggest cloud providers (IaaS) which leads to data theft.
- Breakdown of a popular software (e.g. Microsoft outlook).

Benefits:

- Extreme scenarios considered;
- Transparency;
- Cause-based procedure;
- Ease in results communication for cumulative damage measurements.

Disadvantages:

- Modeling of damage vector (not sure if all damage types are considered);
- Not suitable for expected value calculations;
- Dependence on central assumptions.

Worldwide IaaS Public Cloud Services Market Share, 2017-2018

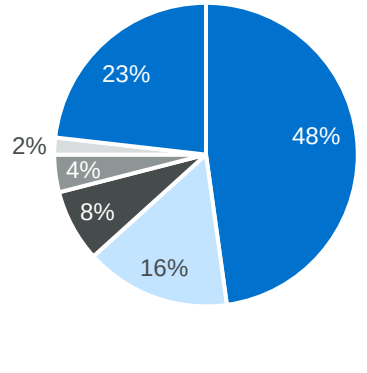
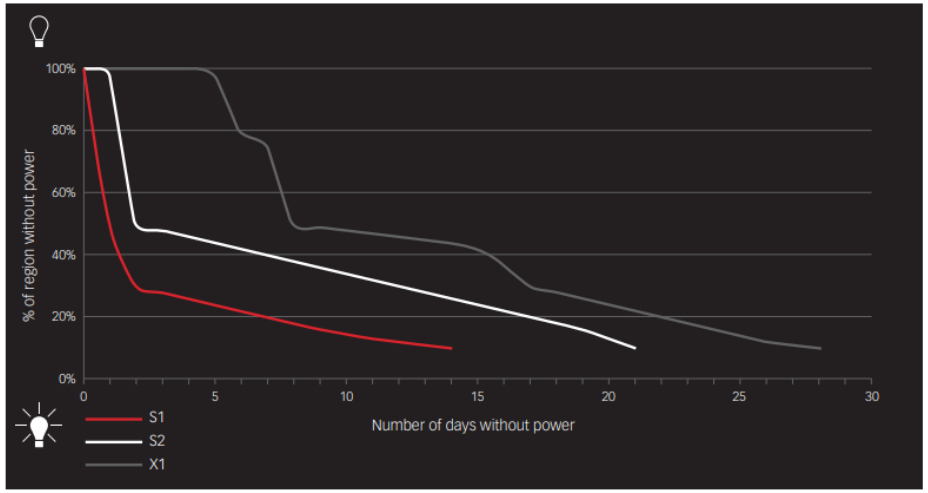


Figure 2: Duration and extent of power outages for each scenario variant



The insurance implications of a cyber attack on the US power
Lloyd's Emerging Risk Report, 2015

Cyber-Risk & Cyber-Governance –… und regulatorischen Herausforderungen **Herausforderung für die Modellierung**

Rolle und Aufgabe des Aktuars / Versicherungsmathematikers in Bezug auf Cyberrisiken:

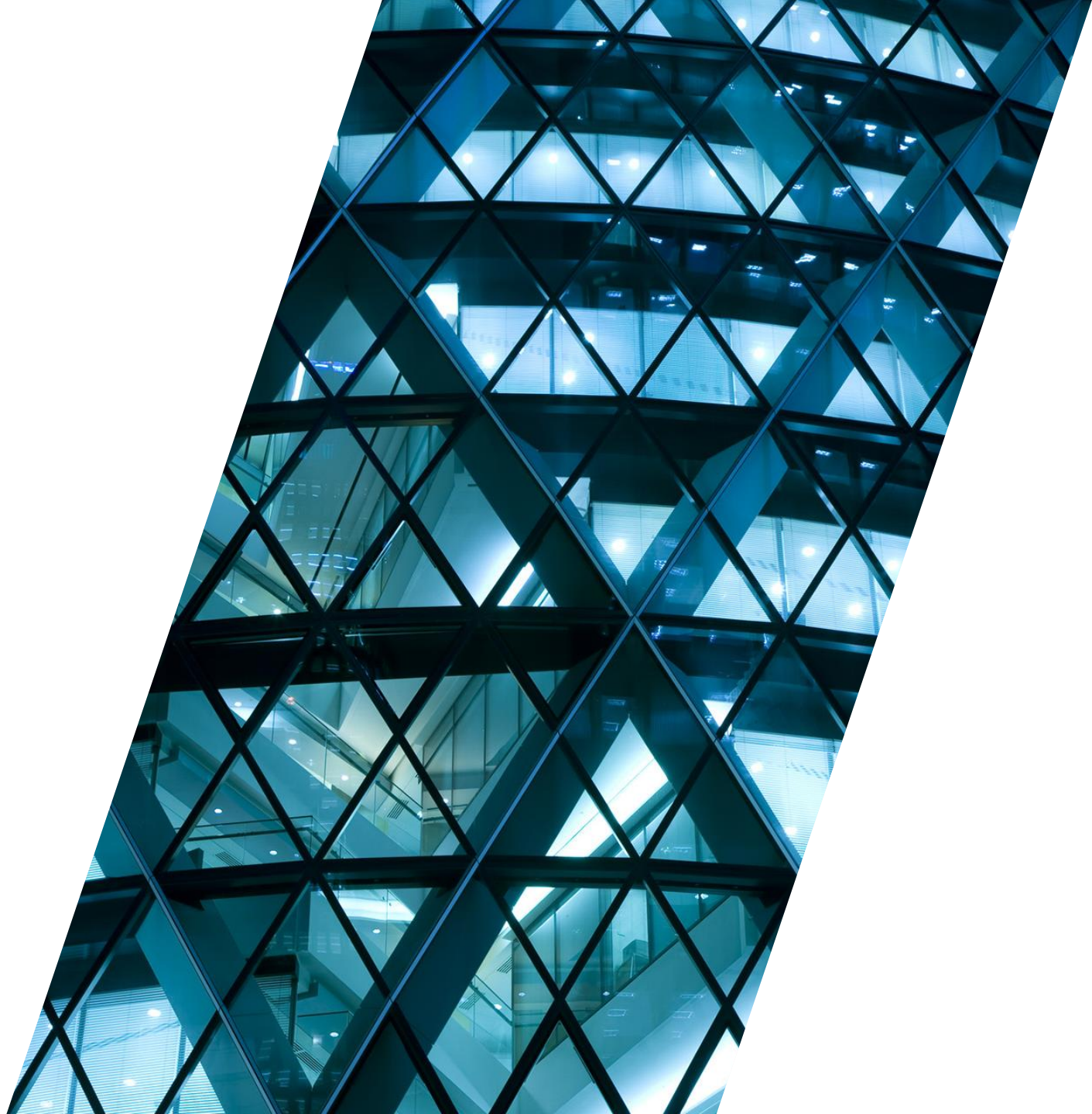
- Methodik der **Risikomessung**
- **Quantifizierung** des Risikos
- Wirkungsstudien und Szenarien
- Beitrag zur Strategie
- **Priorisierung** durch Risikoanalyse. Beleuchten, wo man anfängt.
- IT/IKT wird „nur“ als Werkzeug gesehen – wenn auch ein überlebenswichtiges. **Verpflichtung zur Schulung und Sensibilisierung aller, welche Relevanz und welches Risiko IT/IKT hat.**
- Es liegt an den Fachleuten, ihre Kompetenzen und ihr Risikobewusstsein zu demonstrieren.

Cyber-Risk & Cyber-Governance –… und regulatorischen Herausforderungen

Worum es bisher ging….

04

Ausblick und Zusammenfassung



Cyber-Risk & Cyber-Governance
Ausblick und Zusammenfassung

Marktentwicklung
Produktentwicklung

Chancen und Risiken in einem Emerging Risk Market. Der Trend geht zu einem weiteren Wachstum und das Potenzial dazu ist da. Chancen und Risiken halten sich immer die Waage.

Governance & Regulierung

Herausforderung in der Dokumentation und Definition der bisherigen Begrifflichkeiten der DORA. Weitere Klarstellungen und Interpretationen sind zu erwarten. DORA rückt das Thema aber in einen verbindlichen Zustand.

Aktuarielle Modellierung

Methoden, Annahmen und Projektionen werden sich in den nächsten Jahren signifikant weiterentwickeln, da sowohl die Regulierung als auch die Produktentwicklung dies bedingen.

Forvis Mazars für Forum V – Versicherungsmathematisches Kolloquium

Vielen Dank für Ihre Aufmerksamkeit

Meinolf List
Senior Manager
OneInsurance Forvis Mazars
München

meinolf.list@mazars.de
+49 170 3766 252

Alexandre Extrat
Aktuar (DAV)
Manager
OneInsurance Forvis Mazars
Köln

alexandre.extrat@mazars.de
+49 170 3754 391

Standorte in Deutschland

Berlin
Alt-Moabit 2
10557 Berlin
Tel: +49 30 208 88 0

Dresden
Kleine Brüdergasse 3
01067 Dresden
Tel: +49 351 45 15 0

Düsseldorf
Bennigsen-Platz 1
40474 Düsseldorf
Tel: +49 211 83 99 0

Frankfurt am Main
Theodor-Stern-Kai 1
60596 Frankfurt am Main
Tel: +49 69 967 65 0

Greifswald
Steinbeckerstraße 10
17489 Greifswald
Tel: +49 3834 885 33 40

Hamburg
Domstraße 15
20095 Hamburg
Tel: +49 40 288 01 0

Köln
Im Zollhafen 24
50678 Köln
Tel: +49 221 28 20 0

Leipzig
Hugo-Licht-Straße 3
04109 Leipzig
Tel: +49 341 60 03 0

München
Ridlerstraße 39
80339 München
Tel: +49 89 350 00 0

Nürnberg
Längenstraße 14
90491 Nürnberg
Tel: +49 911 60 07 0

Potsdam
Hebbelstraße 27
14469 Potsdam
Tel: +49 331 73 04 07 70

Stuttgart
Breitscheidstraße 10
70174 Stuttgart
Tel: +49 711 666 31 0

Kontakt

Forvis Mazars

Forvis Mazars GmbH & Co. KG
Wirtschaftsprüfungsgesellschaft
Steuerberatungsgesellschaft
Domstraße 15 | 20095 Hamburg
Tel: +49 40 288 01 0

Follow us

LinkedIn:
Forvis Mazars in Germany

Xing:
Forvis Mazars in Germany

Facebook:
Forvis Mazars in Germany

Instagram:
Forvis Mazars in Germany

Weitere Informationen finden Sie unter www.forvismazars.com/de