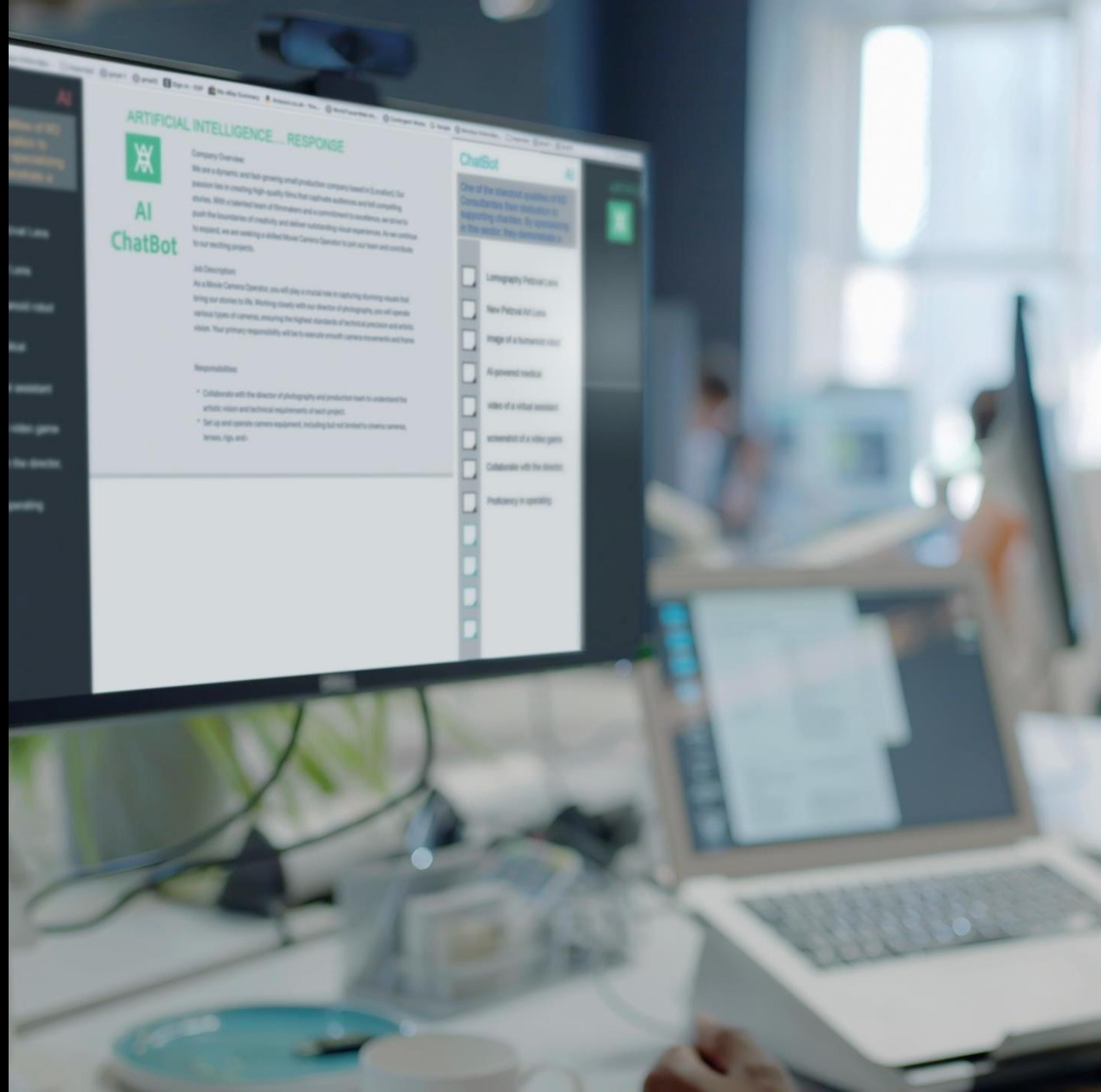
# Cyber Solutions

## Cyber Crime und KI – Ist das noch versicherbar

Wien, 12.06.2025



# 1.

## Aktuelle Schaden- und Risikosituation

ZDNet/Alerts

Hacker nutzen DeepSeek und Qwen zur Entwicklung bösartiger Inhalte

U.S. NEWS

**Man who exploded Tesla Cybertruck outside Trump hotel in Las Vegas used generative AI, police say**

Hacker-Gruppen nutzen Googles KI Gemini für Aufklärung und Angriffsvorbereitung

Staatlich geförderte Hackergruppen missbrauchen Googles KI-gestützten Assistenten Gemini, um potenzielle Angriffsziele zu erforschen.

Heise Online

MIT Technology Review

Cyberattacks by AI agents are coming

Agents could make it easier and cheaper for criminals to hack systems at scale.

MIT Technology Review

**Indiana-Jones-Methode: Forscher zeigen, wie leicht sich KI-Modelle austricksen lassen**

Die Methode nutzt Referenzen zu historischen Personen, um schädliche Informationen aus den LLMs herauszulocken.

ZDNet/Alerts

Ransomware-Gruppe FunkSec setzt auf KI-gestützte Angriffe

«2024 ist das erste Jahr, wo KI nicht nur als hypothetisches Problem wahrgenommen wird, sondern tatsächlich genutzt wird. KI ist endgültig auf der Straftäterseite angekommen», sagte der Leitende Oberstaatsanwalt Thomas Goger, stellvertretender Chef der Zentralstelle Cybercrime Bayern.

[https://www.zeit.de/thema/bayern]

# Aktuelle Schaden- und Risikosituation

AON

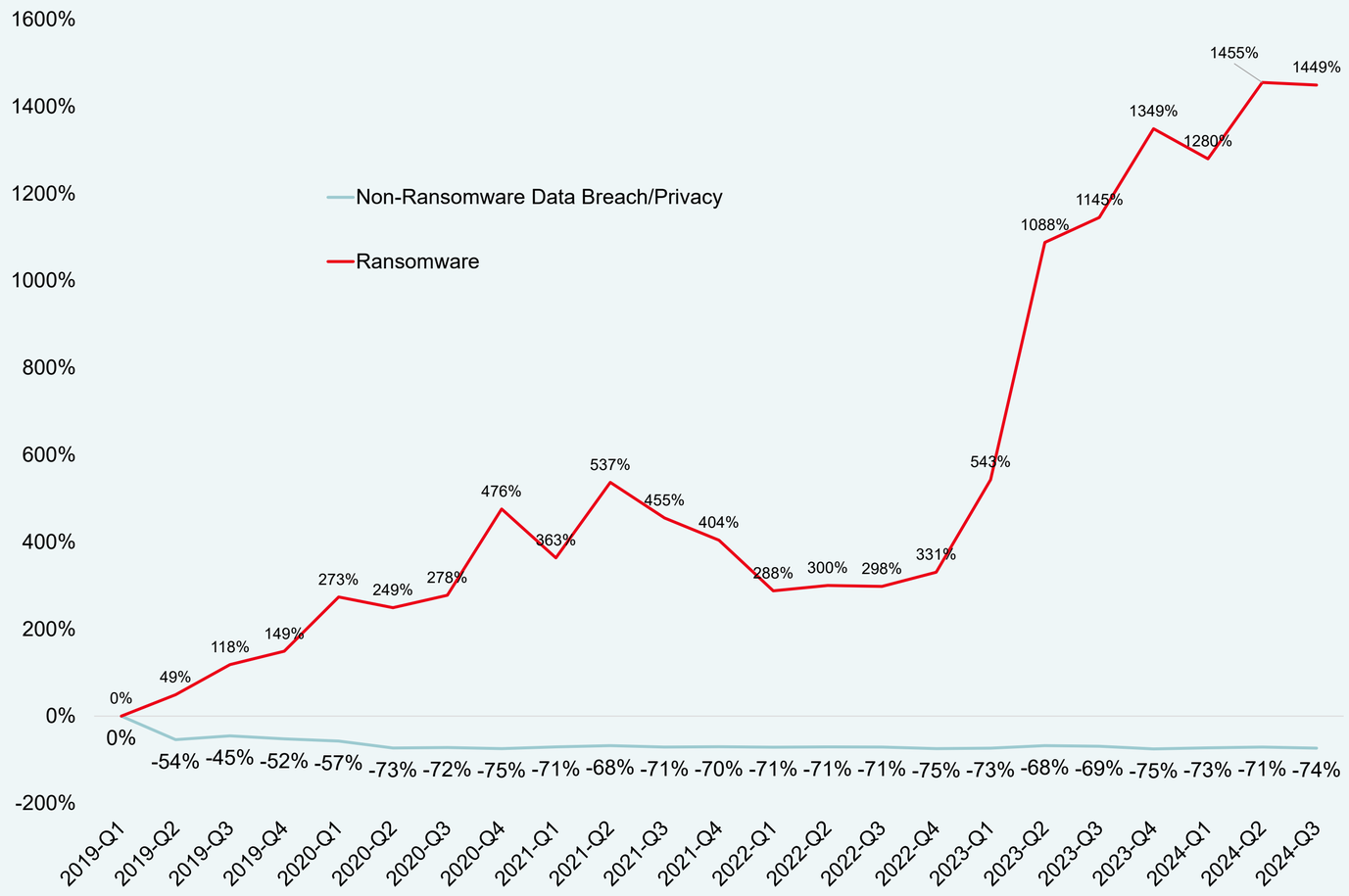
# Schadenentwicklung

**Auszüge aus dem Q4 Risk-Report:**

- Ransomware Ereignisse stiegen von Q3 2024 bis Q4 2024 um 28 %.
- Die am häufigsten von Ransomware betroffenen Regionen in Q4 2024:
  - USA/Kanada
  - West-Europa
- Insgesamt **62 Hacker-Gruppierungen** veröffentlichten im Q4 durch Ransomware ergatterte Daten, ein **Anstieg von 5 Gruppen** gegenüber Q3

**54 %** der **Betriebsunterbrechungen** sind auf System- oder Datenverluste zurückzuführen. Somit sind diese bedeutender als Betriebs-unterbrechungen aufgrund von Ereignissen, die sich auf traditionelle Sachwerte beziehen.

**12%** der österreichischen Unternehmen hatten einen Schaden in Höhe von **über EUR 1 Mio.**




Source: Risk Based Security, analysis by Aon. Data as of 4/1/2024; Claim count development may cause these percentages to change over time

# 2.

## Versicherbarkeit von Cyber Crime und KI-Risiken

# KI Risiken | Versicherungsparten

## Die größten Risiken anhand der Versicherungssparten

### Cyberversicherung

Datenschutz- und Geheimhaltungspflicht-verletzungen durch Nutzung von KI. Prompt Injections und Verwendung von KI als Angriffsmittel.

### Vertrauensschaden-versicherung

KI als Tatwerkzeug für betrügerische Handlungen (Social Engineering Fraud). Durch Nachahmung von Text, Bild und Sprache.

### Produkthaftpflicht

Einsatz von KI in der Produktion kann zu Fehlern im Produktionsprozess und mangelhaften Produkten führen. Produktrückrufe können die Folge sein.

### Technology Errors & Omissions

KI erteilt einen falschen Rat, „Halluziniert“ und liefert unrichtige Informationen, falsche Ableitungen. KI erteilt schädigende Auskünfte.

### Medienrechtsverletzung & Reputationsschaden

KI kann im Bereich des Marketings zu Schäden aufgrund von falschen Werbe-aussagen und Reputationsverletzungen führen.

### Intellectual Property

Urheberrechtsverletzungen durch KI. Unrechtmäßige Nutzung von Bild und Stimme. Verletzung von Marken- und Patenrechten.

### Directors & Officers

Neben den Risiken für Manager durch den Einsatz von KI, rückt auch die Thematik „AI Washing“ immer stärker in den Vordergrund.

### Diskriminierung

Die KI trifft diskriminierende Entscheidung, schließt eine Personengruppe unrechtmäßig aus oder stellt eine Gruppe fälschlicherweise unter Verdacht.

### Personen- und Sachschäden

Durch den Einsatz von Robotik und IoT kann KI als alleiniger Verursacher von Personen- und Sachschäden fungieren. Dies führt rechtlich zu neuen Herausforderungen.

# Abgrenzung | Cyber-Versicherung x VSV

**Zielrichtung Cyber-Versicherung:**

Eingriffe in die IT- und Datensicherheit (Hacker-Angriffe), technische Ausfälle (verbundenes System), Ansprüche aufg. von Datenleaks, technischer und juristischer Support im Schadenfall (24/7 Hotline)

**Zielrichtung Vertrauensschadenversicherung:**

Betrugsfälle ohne vorangegangene Netzwerksicherheitsverletzung (Lieferantenbetrug, Fake-President, Social Engineering) & klassische Vertrauensschäden, z.B. Diebstahl durch eigene Mitarbeiter.

Auslöser

Umfang

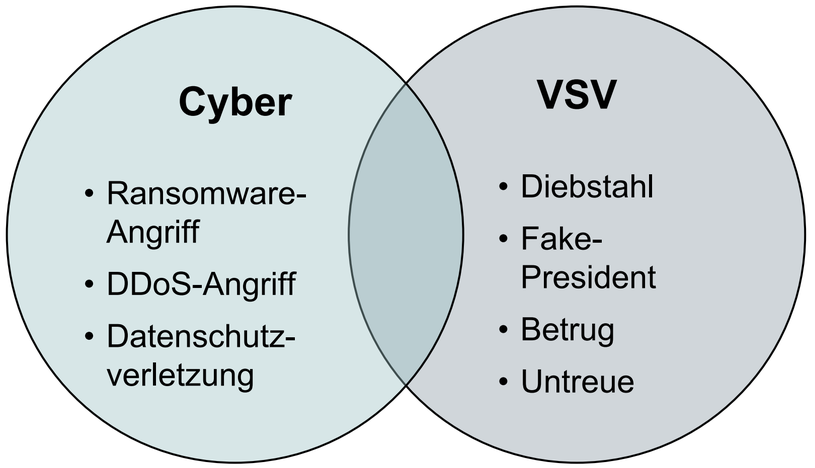
**Auslösende Ereignisse:**

- Eindringen in das versicherte Computersystem (Hackerangriff)
- Fehlbedienung
- Systemausfall
- Datenschutzverletzung

**Deckungselemente:**

- Eigenschäden (entgangene Gewinne, Mehrkosten, Lösegeld)
- Assistance-Leistungen (Krisenreaktion, Rechtsberatung, Lösegeldverhandlungen)
- Haftpflicht (Ansprüche aufg. DSGVO-Verstoß, Bußgelder, Geheimhaltungsverpflichtungen)
- Rechtsschutz

**Polizzentrigger**




**Auslösende Ereignisse:**

- Fake-President
- Betrug (z.B. Lieferanten- oder KI-Betrug)
- Diebstahl
- Unterschlagung
- Bestechung

**Deckungselemente:**

- Versichert ist der finanzielle Schaden = eingetretener Vermögensverlust
- Schadenermittlung- und Rechtsverfolgungskosten
- Kosten für interne Untersuchungen
- Reputationsberatung

Auslöser

Umfang

Die VSV leistet nach Schäden, die vorsätzlich durch kriminelle Mitarbeiter und durch Außenstehende herbeigeführt werden:

- Der durch Wirtschaftskriminalität erfasste **finanzielle Schaden** lag 2023 bei **EUR 2,679 Mrd.** (+ 28,6% zum Vorjahr).*
- **Cyber-Versicherung und VSV**: Kombination bietet **umfassenden Versicherungsschutz** gegen Betrugsszenarien.

AON



*Quelle: Bundeslagebild Wirtschaftskriminalität 2023

# KI | Herausforderungen für die Versicherbarkeit

## Fehlende Standardisierung:

Die starken und dynamischen Entwicklungen im Bereich der künstlichen Intelligenz stellen die Versicherungswirtschaft vor große Herausforderungen. Die Konzipierung von Produkten ist aufgrund der fehlenden Standardisierung kaum möglich.

## Unklarheit über den Versicherungsumfang:

Die KI-Revolution erinnert stark an den Beginn der Cyberversicherung. Auch diesmal ist der Versicherungsumfang der bestehenden Produkte in Hinblick auf die neue Risikosituation fraglich. Sogenannte „Silent KI-Deckungen“ finden sich in vielen altbewährten und auch jüngeren Versicherungs-produkten. Wie bereits bei der Cyberversicherung führen diese Deckungen im Schadenfall oftmals zu Deckungsstreitigkeiten und sind aus diesem Grund mit Vorsicht zu behandeln.

## Wachsende Risiken durch KI:

Basierend auf den enormen Kapazitäten von KI entsteht eine vollkommen neuartige Risikosituation. Der Versicherungsschutz für diese Risiken muss aus diesem Grund öfter überprüft und angepasst werden.

## Komplexe Schadenabwicklung:

Die Schadenabwicklung von KI Schäden stellt alle Beteiligten vor große Herausforderungen, neben den vielen Beteiligten führt oftmals auch die Haftung zu komplexen Rechtsfragen.

## KI Spezielle Versicherungsangebote

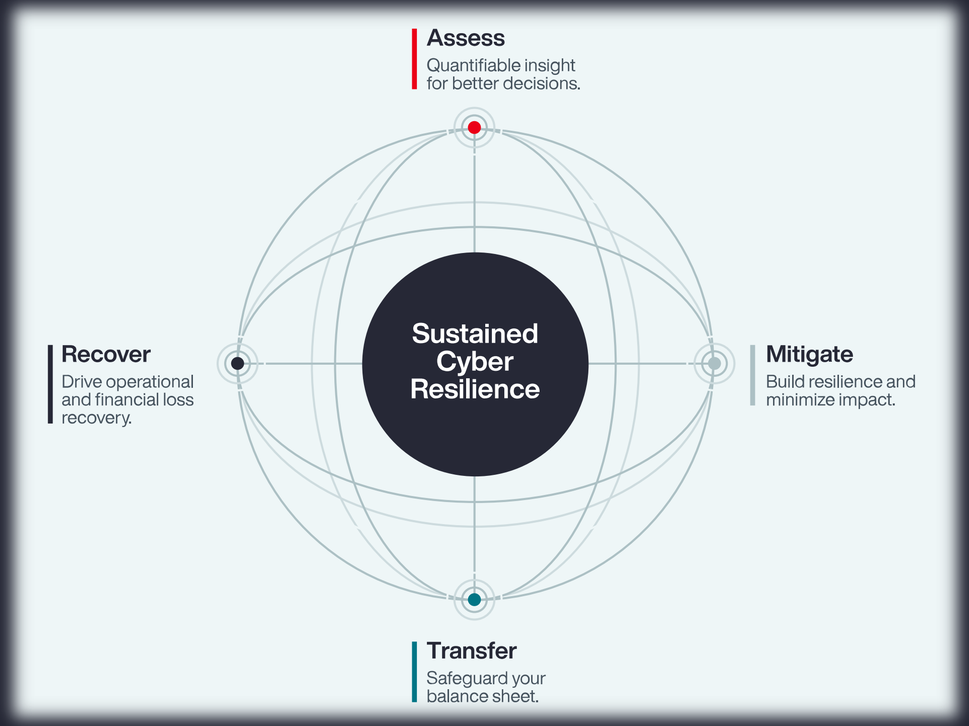
- Munich Re stellt eine KI Performance Versicherungslösung zur Verfügung
- AXA XL vergrößert den Deckungsumfang ihrer bestehenden Cyberversicherungslösung auf KI-Risiken
- Coalition bietet Versicherungsmaklern und Endkunden KI-Tools zur proaktiven Absicherung an
- Armilla AI | bietet sowohl proaktive als auch reaktive Lösungen für KI-Risiken
- Artificial Intelligence Liability Insurance | Haftpflichtversicherung für KMU‘s
- Move faster with AI Insurance | Haftpflichtversicherung für KMU‘s
- Relm Insurance offeriert spezielle KI-Versicherungslösungen
  - NOVAAI  ist eine Cyber und Tech E&O-Versicherung für Anbieter von KI-Lösungen.
  - PONTAAI  wurde als “AI-Wrap” konzipiert und stellt eine Umbrella-Lösung, für Unternehmen die KI-Lösungen nutzen und nicht selbst kreieren, dar.
  - RESCAAI ist eine Eigenschadenversicherung, mit Fokus auf Incident Response für Unternehmen, die eine KI-Lösung von einer Drittpartei beziehen, um ihre Betriebstätigkeit damit auszuüben, beispielsweise Online-Händler oder die diese KI-Lösungen in ihre Produkte einbauen, wie beispielsweise Spielzeug- oder Autohersteller.

# KI Risiken | Versicherbarkeit im Überblick

| KI-Risiko | Medien-haftpflicht | Berufs-haftpflicht | Produkt-haftpflicht | Betriebs-haftpflicht | Geistiges Eigentum | Cyber | Vertrauens-schaden | D&O |
|---|---|---|---|---|---|---|---|---|
| Haftung für fehlerhafte Produkte und Dienstleistungen | ● | ● | ● | ● | ● | ● | ● | ● |
| Urheberrecht, Marken- oder Dienstleistungsmarkenverletzung | ● | ● | ● | ● | ● | ● | ● | ● |
| Patentrechtsverletzung | ● | ● | ● | ● | ● | ● | ● | ● |
| Diskriminierung/ Voreingenommenheit | ● | ● | ● | ● | ● | ● | ● | ● |
| Verleumdung, üble Nachrede, Beleidigung | ● | ● | ● | ● | ● | ● | ● | ● |
| Personenschäden | ● | ● | ● | ● | ● | ● | ● | ● |
| Sachschäden | ● | ● | ● | ● | ● | ● | ● | ● |
| Datenschutz- und Sicherheitsverletzungen | ● | ● | ● | ● | ● | ● | ● | ● |
| Verlust finanzieller Vermögenswerte | ● | ● | ● | ● | ● | ● | ● | ● |
| Marktmanipulation | ● | ● | ● | ● | ● | ● | ● | ● |
| Täuschung | ● | ● | ● | ● | ● | ● | ● | ● |
| Robotik | ● | ● | ● | ● | ● | ● | ● | ● |
| Produktrückruf | ● | ● | ● | ● | ● | ● | ● | ● |
| Betriebsunterbrechung | ● | ● | ● | ● | ● | ● | ● | ● |
| Verletzung der Pflichten von Führungskräften | ● | ● | ● | ● | ● | ● | ● | ● |

● Allgemein verfügbar ● Limitiert ● Ausgeschlossen

# Ich freue mich auf einen Austausch mit Ihnen!




**Mag. Kerstin Keltner**
Managing Director Specialty

+43 676 5955424
kerstin.keltner@aon-austria.at