



Whitepaper

# **UNTERNEHMENSRISENEN 2026: WO DIE GEFAHREN RICHTIG BRENNEN**

**Crisis Heat Map Q4/2025  
von Sieber Advisors**

Von Dr. Armin Sieber, Sieber Advisors

## 1. Einleitung

Die Lage für Unternehmen bleibt angespannt. Globale Spannungen, KI-getriebene Angriffsformen, Lieferkettenbrüche und politisch induzierte Unsicherheiten verschärfen sich. Die neue **Crisis Heat Map Q4/2025** zeigt, wo sich Risiken verdichten – und welche Themen 2026 den Ausschlag geben könnten.

**Halbjährliches Update**

Im Mittelpunkt steht die Visualisierung: Sie verdichtet 20 Krisenrisiken aus ökonomischer und reputativer Sicht zu einem Lagebild der Unternehmensrisiken – einem **Radar für kommunikative Verwundbarkeit**.

## 2. Die Crisis Heat-Map im Überblick

Sieber Advisors erhebt halbjährlich die Top-Risiken für Unternehmen. Die Crisis Heat Map basiert auf einer kombinierten Bewertung von:

- **Ökonomischem Schaden (Y-Achse)**
- **Reputationsschaden (X-Achse)**

Aus beiden Achsen entsteht ein **Indexwert**, der Trends über Zeit sichtbar macht. Grundlage der Analyse sind internationale Risiko-Reports (u.a. Allianz, WEF, PwC, DIIR, KPMG) sowie reale Krisenfälle der Gegenwart.

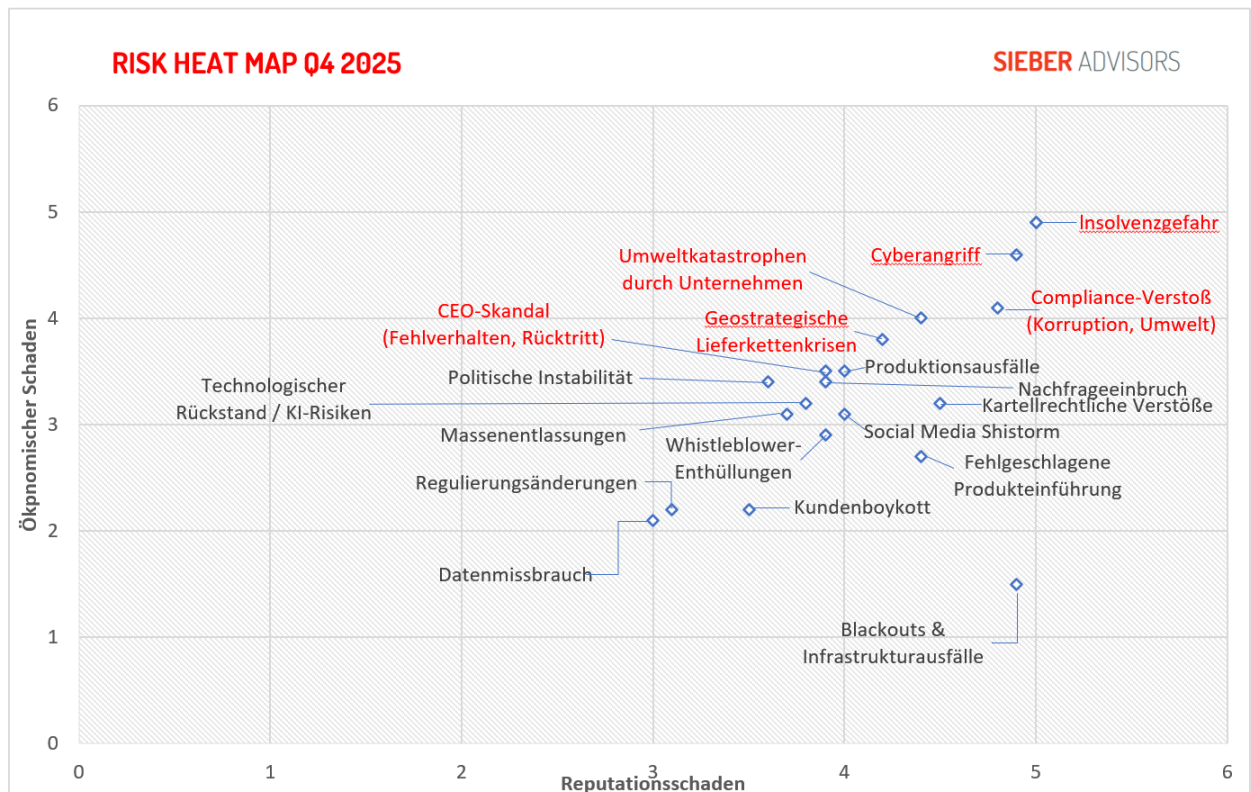
**Metastudie plus Medienanalyse**

Die aktuelle Auswertung zeigt eine **Massierung kritischer Risiken im Hochrisikouadranten** – mit Cyber, Insolvenz und Geostrategie an der Spitze.

**„Resilienz entsteht nicht durch Robustheit, sondern durch Lernfähigkeit.“**

2026 wird kein Jahr einzelner Großereignisse, sondern eines kumulativen Risiko-Clashes. Unternehmen, die Risiken nur sektoral managen, unterschätzen die Interdependenzen. Entscheidend ist, die Schnittstellen zu verstehen – zwischen IT, Politik und Reputation.

Die Unternehmen, die 2026 erfolgreich sein werden, sind nicht die, die alle Risiken ausschließen, sondern die, die sie verstehen, antizipieren und erzählerisch einordnen können.



### 3. Die Top 6 Risiken Q4/2025

- (1) **Cyberangriff** – bleibt das strukturelle Top-Risiko. Angriffe werden koordinierter, KI-gestützt und reputationswirksam.
- (2) **Insolvenzrisiko** – scharfe Zinsphase und geopolitische Unsicherheiten erhöhen den Druck.
- (3) **Compliance-Verstöße (Korruption, Umwelt)** – steigende ESG-Erwartungen verschärfen Haftungsrisiken.
- (4) **Geostrategische Krisen / Lieferketten** – Top-Aufsteiger-Risiko (+1,02 Punkte). Konflikte, Handelskriege und Blockaden bedrohen Stabilität.
- (5) **Umweltkatastrophen durch Unternehmen** – Greenwashing-Fälle und Klimaverantwortung rücken stärker in die Öffentlichkeit.
- (6) **CEO-Skandale** – Vertrauensrisiko durch Fehlverhalten oder Rücktritte im Top-Management

## 4. Veränderungen gegenüber Q1/2025

Die Indexvergleiche zeigen klare Verschiebungen:

- **Geostrategische Risiken** legten um durchschnittlich +1,3 Punkte zu – die stärkste Bewegung im gesamten Ranking.
- **Cyber- und Insolvenzrisiken** liegen nahezu gleichauf und bleiben im Hochrisikobereich stabil.
- **Compliance-Themen** und **CEO-Skandale** steigen leicht, getrieben durch öffentliche Debatten um Integrität und Governance.

**Stärkster Anstieg**

Diese Trends markieren einen Übergang von Einzelfällen zu Systemrisiken – besonders dort, wo Technologie, Politik und Reputation ineinandergreifen.

## 5. Schlüsseleinsichten und Ausblick 2026

Die Crisis Heat Map Q4/2025 zeigt: Die Risikolandschaft verdichtet sich in drei zentralen Clustern – **Cyber, Geostrategie & Lieferketten, Governance & Compliance**. Sie sind nicht mehr isolierbar, sondern haben das Potenzial sich zu Polykrisen zu verdichten.

### 5.1. Cyber als systemisches Risiko

Cyberangriffe sind längst keine technischen Vorfälle mehr, sondern Kommunikations- und Vertrauenskrisen mit globaler Dimension.

- **Neue Akteure, neue Taktiken:** Staatlich gesteuerte Gruppen (GRU) agieren arbeitsteilig und KI-gestützt. Generative KI ermöglicht täuschend echte Phishing-Mails, Deep-Fake-Identitäten und manipulative Desinformationskampagnen.
- **Verzahnung von Angriff und Kommunikation:** Jede technische Störung wird durch die öffentliche Wahrnehmung verstärkt. Ein IT-Incident kann in Stunden zum Reputationsschaden werden.
- **Implikation:** Für Unternehmen wird Cyber-Resilienz zur integralen Aufgabe – nicht nur der IT, sondern auch der Kommunikation.
  - **Frühwarnsysteme und KI-gestützte Monitoring-Tools** müssen auf kommunikative Signale reagieren.
  - **Krisenpläne** sollten den „Übergangspunkt“ vom IT-Vorfall zur Kommunikationskrise abbilden.

## 5.2. Geostrategische Risiken und Lieferketten

Das Top-Aufsteiger-Risiko 2025 (+ 1,02 Indexpunkte) betrifft die Verwundbarkeit globaler Strukturen.

- **Zoll- und Handelspolitik:** Der faktische Wirtschaftskrieg zwischen USA, Europa und China führt zu neuen Unsicherheiten in Absatz- und Beschaffungsmärkten.
- **Regionale Konflikte:** Der Krieg in der Ukraine, Spannungen im Baltikum, Taiwan und im Nahen Osten wirken als multiple Schocks auf Transport-, Energie- und Rohstoffströme.
- **Systemische Effekte:** Lieferketten sind nicht mehr linear, sondern fragmentiert. Jede Störung erzeugt Nachbeben entlang der gesamten Wertschöpfung.
- **Implikation:** Unternehmen müssen ihre Kommunikations- und Entscheidungsstrukturen geografisch diversifizieren:
  - **Szenarien und Redundanzen** in der Beschaffung transparent kommunizieren.
  - **Stakeholder-Dialoge** auf geopolitische Spannungen vorbereiten – etwa über regionale Risiko-Briefings und faktenbasierte Narrative zu Versorgungssicherheit.

## 5.3. Governance, Compliance und Integrität

ESG- und Governance-Themen wandeln sich vom Reputationsfaktor zum Haftungsrisiko.

- **Strengere Regulatorik:** EU-Lieferkettengesetz, NIS-2-Richtlinie und verschärfte ESG-Berichtspflichten erhöhen die persönliche Verantwortung von Vorständen.
- **Mediale Aufmerksamkeit:** Whistleblower-Enthüllungen und Investigativ-Formate erzeugen eine neue Transparenzkultur.
- **Implikation:** Reputationsschutz beginnt bei Governance.
  - **Interne Kontrollsysteme** müssen kommunikativ anschlussfähig werden.
  - **Compliance-Krisen** sollten wie Produkt- oder IT-Krisen strukturiert vorbereitet werden – mit klaren Eskalationspfaden und dokumentierten Reaktionsmechanismen.

## Fazit

### Kumulative Risiko Cluster

2026 wird kein Jahr einzelner Großereignisse, sondern eines kumulativen Risiko-Clashes. Unternehmen, die Risiken nur sektoral managen, unterschätzen die Interdependenzen. Entscheidend ist, die Schnittstellen zu verstehen – zwischen IT, Politik und Reputation.

## 6. Kontakt

Möchten Sie mehr darüber erfahren, wie Ihr Unternehmen sich auf die neuen Risiken 2026 vorbereiten kann?

Kontaktieren Sie uns für eine unverbindliche Beratung.

### **Dr. Armin Sieber**

Telefon +49 89 99 27 58 46

Mobil: +49 172 147 34 92

Mail: [armin.sieber@sieber-advisors.de](mailto:armin.sieber@sieber-advisors.de)

