beazley

Spotlight: Tech-Transformation & Cyber-Risiken 2025

Europa Daten: Fokus Deutschland

Spotlight: Cyber- & Tech-Risiken

Die diesjährige Umfrage wurde zwischen dem 06.01.25 und dem 17.01.25 durchgeführt. Im Jahr 2021 wurde die Umfrage unter Befragten mit Sitz im Vereinigten Königreich und in den Vereinigten Staaten durchgeführt. In den Jahren 2022 und 2023 umfasste die Stichprobe auch Befragte aus Kanada und Singapur, und im Jahr 2024 wurde die Stichprobe erweitert, um auch Befragte aus Frankreich, Deutschland und Spanien einzubeziehen.

beazley

Wir haben 3500 globale Führungskräfte gefragt, ...

was ihre größten Geschäftsrisiken sind und wie resilient sie sich gegenüber den folgenden Risiken fühlen: ...

- Cyber
- Disruptive Technologien
- Technologische Obsoleszenz
- Geistiges Eigentum (IP)

Wir haben diese Forschung im Januar 2025 mit globalen Geschäftsführern (Versicherungskäufern) aus verschiedenen Branchen durchgeführt:

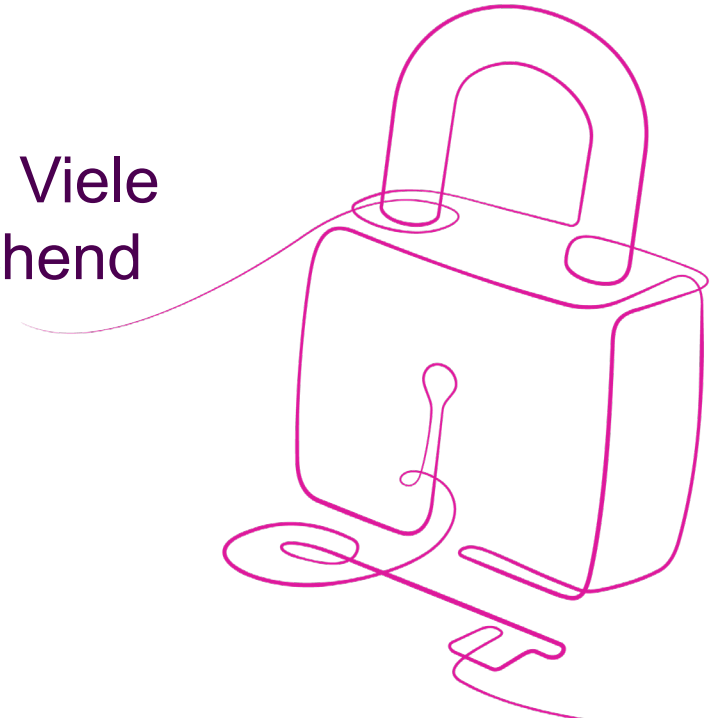
- Gesundheitswesen und Life Sciences
- Fertigung, Einzelhandel, Food & Beverage
- Immobilien & Bau
- Unterhaltung, Gastgewerbe und Freizeit (einschließlich Gaming)
- Finanzinstitute und professionelle Dienstleistungen
- Energie (einschließlich Bergbau), Infrastruktur, Schifffahrt und Warenlager
- Öffentlicher Sektor und Bildungswesen
- Technologie, Medien und Telekommunikation
- Transport, Logistik, Fracht und Luftfahrt

Wahrnehmung

Die Sorge um Cyber- und Tech-Risiken nimmt zu. Doch Führungskräfte fühlen sich besser auf diese Risiken vorbereitet.

Realität

Digitale Bedrohungen entwickeln sich rasant weiter. Viele Unternehmen sind ihnen ausgesetzt – und unzureichend darauf vorbereitet.



Deutsche Unternehmen stehen einer regelrechten **‚Mäusejagd'** an Cyber- und Tech-Risiken gegenüber, die ein wachsames und umfassendes Risikomanagement erfordert.

Unternehmen benötigen Unterstützung bei der Umsetzung von **‚Defence-in-Depth'**-Strategien, um ihre Resilienz zu stärken

30%

der Befragten erkennen Cyber-Risiken im Jahr 2025 als größte Bedrohung an – ein Anstieg gegenüber 28 % im Jahr 2024. Trotzdem fühlen sich 87 % gut darauf vorbereitet – ein Anstieg gegenüber 81 % im Jahr 2024.*

82%

geben an, dass ihr Unternehmen plane, die Cybersicherheit in Bezug auf Drittanbieter zu verbessern – als Reaktion auf prominente, systemische Cybervorfälle.

38%

planen, in diesem Jahr in eine verbesserte Cybersicherheit zu investieren – ein Anstieg gegenüber 28 % im Jahr 2024.

77%

stimmen zu, dass künstliche Intelligenz in diesem Jahr positive Auswirkungen auf wirtschaftliche Perspektiven ihres Unternehmens haben werde, während 68 % zustimmten, dass KI in den nächsten 18 Monaten Arbeitsplätze in ihrem Unternehmen ersetzen werde.

23%

stufen das Risiko technologischer Obsoleszenz in diesem Jahr als ihr größtes Cyber- und Tech-Risiko ein – im Vergleich zu 27 % im Jahr 2024.

23%

stufen das IP-Risiko in diesem Jahr als größte Bedrohung ein – ein Anstieg gegenüber 21 % im Jahr 2024. Gleichzeitig fühlen sie sich resilienter gegenüber dem IP-Risiko: Nur 15 % fühlen sich unvorbereitet, verglichen mit 21 % im Jahr 2024.**

* Antworten, die ‚sehr gut vorbereitet' und ‚mäßig gut vorbereitet' umfassen.
** Antworten, die ‚nicht besonders gut vorbereitet' und ‚überhaupt nicht vorbereitet' umfassen.

beazley

Unsere Daten zeigen:

- Viele Unternehmen überschätzen ihre Resilienz gegenüber Cyber- und Tech-Risiken.
- Zahlreiche Organisationen sind unzureichend auf Cyberangriffe oder Datenschutzverletzungen vorbereitet.
- Unternehmen wollen ihre Cybersicherheit verbessern.
- Der Optimismus hinsichtlich der Geschäftsvorteile von KI wächst.
- Die Sorge um das Risiko der technologischen Obsoleszenz nimmt ab.

Die wichtigsten Erkenntnisse

Für Broker

1. **Cyber-Resilienz: mehr als Cyberversicherung**
Zusätzlich zum Abschluss einer Cyberversicherung brauchen Unternehmen mehrschichtige Cybersicherheit und eine präventive, reaktionsfähige und anpassungsfähige Unterstützung, die ihnen vor, während und nach einem Cybervorfall hilft, zusätzlich zum Abschluss einer Cyberversicherung.

2. **Erst- und Dritthaftung**
Vernetzte Technologien von heute schaffen Schwachstellen bei Anbietern, die zu Erst- und Dritthaftung führen können: von Cyber-Risiken und Betriebsunterbrechungen bis hin zu D&O- und Reputationsschäden.

3. **Politische Spannungen erhöhen das Cyber-Risiko**
Wenn geopolitische Spannungen zunehmen und sich Beziehungen verschieben, erhöht sich auch das Cyber-Risiko: nationalstaatliche Angreifer schaffen neue Cyber-Schwachstellen, die Cyber-Kriminelle ausnutzen können.

Für Unternehmen

1. **Eine wachsende Sorge für Aktionäre**
Mit dem Cyber-Risiko wächst auch das Risiko von Betriebsunterbrechungen und Rufschädigung. Schlechte Entscheidungen im Bereich Cybersicherheit werden jetzt genauer unter die Lupe genommen, was rechtliche, finanzielle und betriebliche Konsequenzen haben kann.

2. **Alle Augen auf IP-Risiken und Datenschutz**
Nationale IP- und Datenschutzbestimmungen sind fragmentiert und bergen Risiken für international tätige Unternehmen, die unbewusst gegen neue Gesetze verstoßen könnten.

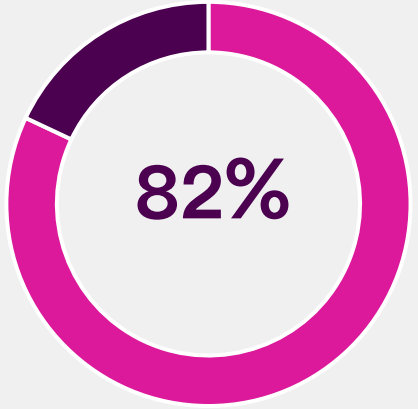
3. **Das Potenzial von KI nutzen**
37% der Führungskräfte weltweit planen in diesem Jahr Investitionen in neue Technologien, und **68 %** rechnen in den nächsten 18 Monaten mit einem KI-bedingten Arbeitsplatzabbau – Unternehmen müssen sich über Best Practices und neue KI-Risiken auf dem Laufenden halten.

Das Trugbild der Cybersicherheit

Weltweit stehen Unternehmen einer ständigen ‚Mäusejagd' von Cyber- und Tech-Risiken gegenüber.

Anfällige Verbindungen

- Das Cyber-Risiko durch Drittanbieter nimmt zu, da Lieferketten zunehmend digital vernetzt sind. Dadurch steigt die Anfälligkeit für Cyberangriffe.
- Cyberkriminelle nehmen große Unternehmen ins Visier, indem sie kleinere Zulieferer angreifen, denen oft Ressourcen für eine robuste Cybersicherheit fehlen.
- Das Auslagern der Cybersicherheit kann ein trügerisches Sicherheitsgefühl vermitteln und ersetzt nicht die Notwendigkeit von:
  - aktivem Mitarbeitertraining
  - einer Business-Continuity-Planung
  - internen Best Practices
  - Defence-in-depth-Cybersicherheit.



deutscher Führungskräfte stimmen zu, dass ihr Unternehmen plane, die Cybersicherheit in Bezug auf Drittanbieter zu verbessern – als Reaktion auf jüngste, prominente systemische Cybervorfälle.

beazley

Das Trugbild Cybersicherheit

Staatliche Akteure setzen Cyberangriffe als Form der Cyberkriegsführung ein, und künstliche Intelligenz (KI) macht Cyberkriminelle noch effektiver.

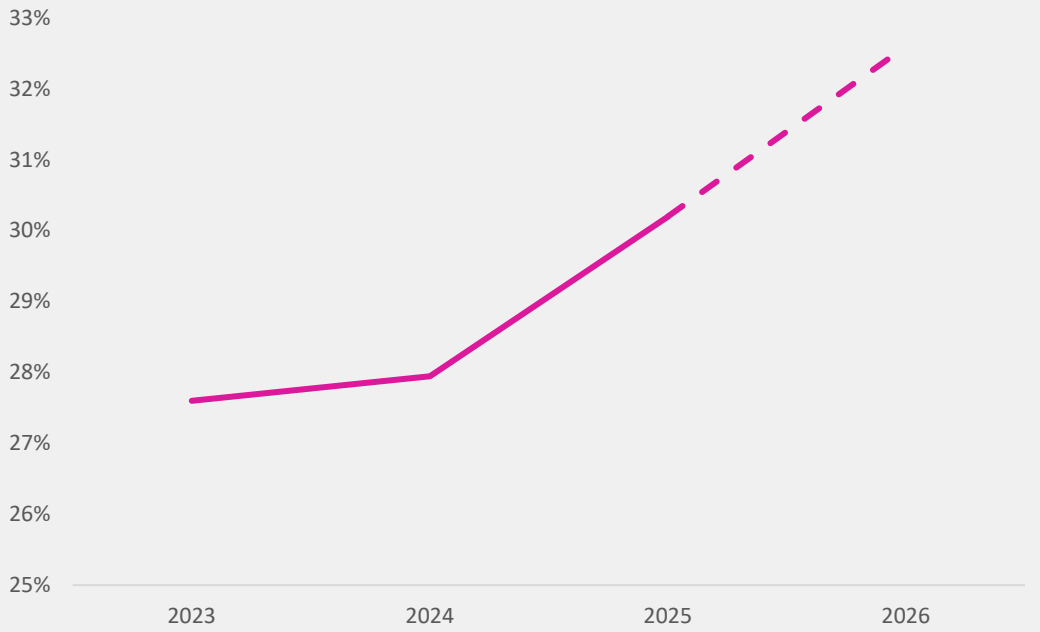
Die Schnittstelle zwischen Politik und Cybersicherheit

- Cyberangriffe sind heute ein Mittel hybrider Kriegsführung. Sie werden eingesetzt, um Störungen zu verursachen und politischen Druck auszuüben.
- Hacktivisten setzen Cyberangriffe ein, um ihre politischen oder sozialen Ziele durchzusetzen – oft bleiben sie dabei lange in Systemen unentdeckt und stellen daher eine langfristige Bedrohung dar.

Ransomware Evolution

- Die Verbreitung von Edge-Geräten und dem Internet der Dinge (IoT) eröffnet Cyberkriminellen neue Einstiegspunkte in Systeme.
- KI hilft Cyberkriminellen dabei, Angriffe zu automatisieren, Phishing zu verbessern und überzeugendere Deepfakes zu erstellen.

Besorgnis über Cyberrisiken im Laufe der Zeit



Der Prozentsatz der in Deutschland ansässigen Führungskräfte, die das Cyberrisiko – also das Versäumnis des Unternehmens, den Datenschutz zu gewährleisten, oder externe kriminelle Bedrohungen wie Ransomware oder umfassendere systemische Bedrohungen, die zu erheblichen Geschäftsunterbrechungen führen – im Laufe der Zeit als ihr größtes Risiko im Bereich Cyber und Technologie eingestuft haben. Die Zahlen für 2026 stellen eine Prognose für das wichtigste Risikothema in den kommenden 12 Monaten dar.

beazley

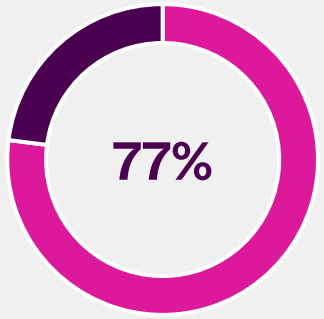
Tech Transformation - vom Code zur digitale Wahrnehmung

Künstliche Intelligenz zwingt Unternehmen dazu, ihre Vorteile gezielt zu nutzen und gleichzeitig wirksame Schutzmaßnahmen gegen neue Risiken zu ergreifen.

Risiko und Chance

Der Optimismus gegenüber KI nimmt stark zu. Heute überwiegt das Risiko, zu wenig in KI zu investieren, gegenüber dem Risiko, zu viel zu investieren.

- Menschliche Kontrolle ist entscheidend, um Risiken wie Urheberrechtsverletzungen, Verletzungen geistigen Eigentums (IP), Voreingenommenheit und Verleumdung zu mindern.

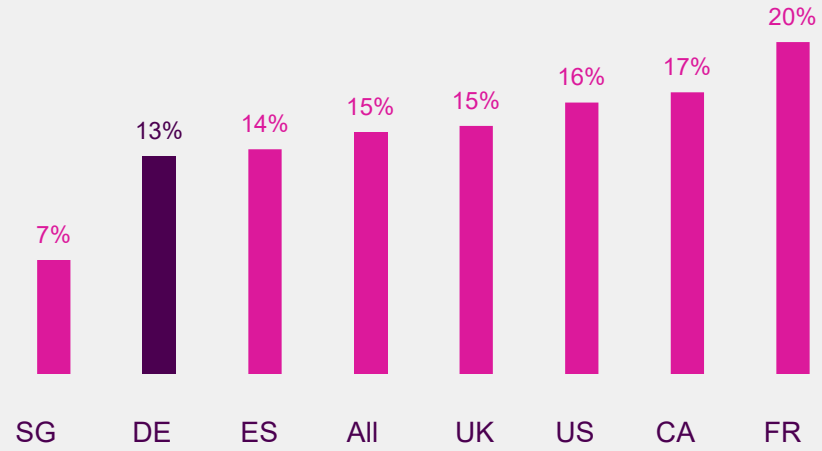


der in Deutschland ansässigen Führungskräfte stimmen zu, dass KI in diesem Jahr einen positiven Einfluss auf die geschäftlichen Aussichten ihres Unternehmens haben wird.

Veraltete Technologien

- KI wirft Bedenken hinsichtlich technologischer Obsoleszenz, Disruption und abnehmender Wettbewerbsfähigkeit auf.

Die Vorbereitung auf technologische Obsoleszenz variiert je nach Region



Der Prozentsatz der Führungskräfte, die sich unvorbereitet fühlen (Kombination der Antworten „nicht sehr gut vorbereitet“ und „überhaupt nicht vorbereitet“), um auf das Risiko technologischer Obsoleszenz zu reagieren – also das Versäumnis, mit der technologischen Entwicklung und neuen Chancen (z. B. generative KI, IoT und Automatisierung) Schritt zu halten oder Systeme zu aktualisieren – als ihr größtes Cyber- und Technologierisiko, aufgeschlüsselt nach Regionen.

beazley

Gesichert oder ungeschützt – IP & Datenschutz

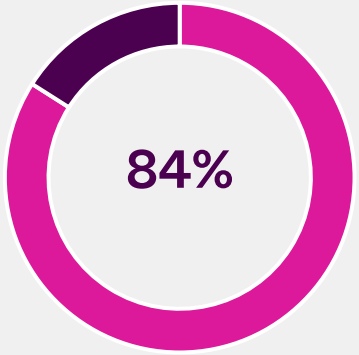
Der Schutz von Daten und die Sicherung geistigen Eigentums sind zunehmend wichtiger geworden.

Versteckte Risiken

Vorschriften rund um KI und Urheberrecht sind nach wie vor unklar, und das Risiko des Diebstahls bestehenden geistigen Eigentums ist erheblich.

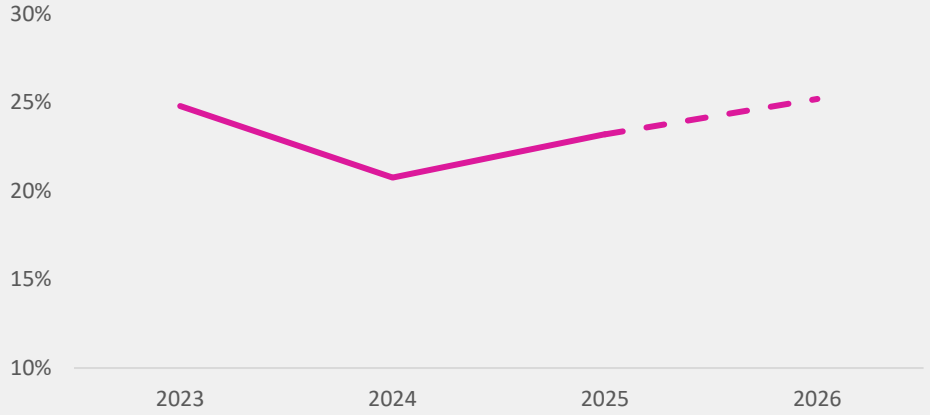
Regulatorischer Flickenteppich

- Neue Vorschriften für Datensicherheit und den Schutz von geistigem Eigentum in verschiedenen Regionen schaffen zusätzliche Komplexität für international tätige Unternehmen.
- Da geopolitische Spannungen anhalten, sind Organisationen dem Risiko von Diebstahl geistigen Eigentums und Datenlecks durch feindlich gesinnte Regierungen ausgesetzt.



der in Deutschland ansässigen Führungskräfte hat einen toten Winkel in Bezug auf Risiken für geistiges Eigentum, obwohl die wahrgenommene Resilienz seit 2024 von 79 % gestiegen ist – und das trotz zunehmender Besorgnis.

Sprunghafter Anstieg der Besorgnis über IP-Risiken in Deutschland in 2025



Der Prozentsatz der in Deutschland ansässigen Führungskräfte, die das Risiko im Bereich geistiges Eigentum – also das Versäumnis, den Wert von IP-Vermögenswerten wie Know-how, Patenten oder immateriellen Gütern zu erkennen und zu schützen – im Laufe der Zeit als ihr größtes Cyber- und Technologierisiko eingestuft haben. Die Zahlen für 2026 stellen eine Prognose für das wichtigste Risikothema in den kommenden 12 Monaten dar.

beazley

Resilienz aufbauen

Die Notwendigkeit eines mehrschichtigen, tiefgreifenden Verteidigungsansatzes in der Cybersicherheit war noch nie so groß wie heute.

Mauern hinter Mauern

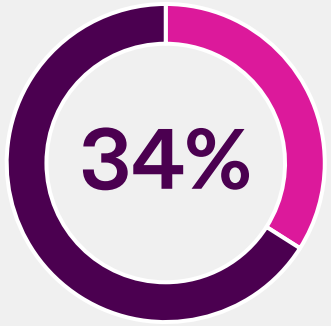
- Mehrere Verteidigungsschichten zum Schutz von Systemen und Daten sicherzustellen, ist von entscheidender Bedeutung.
- Organisationen benötigen eine maßgeschneiderte „Defence-in-Depth“-Strategie, die ihre individuelle Supply Chain und ihr spezifisches Risikoprofil berücksichtigt.

Bedrohungen durch Dritte

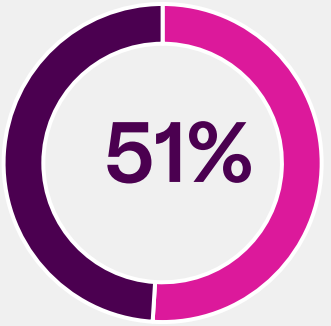
- Verträge mit Drittanbietern können die Haftung des Anbieters einschränken. Das bedeutet, dass Unternehmen im Ernstfall selbst für rechtliche Folgen und finanzielle Schäden durch Angriffe oder Ausfälle bei ihren Dienstleistern aufkommen müssen.

Cyber-Hygiene optimieren

- Gute Cybersicherheit bedeutet, Risiken frühzeitig zu erkennen, schnell auf Bedrohungen zu reagieren und sich flexibel an neue Gefahren anzupassen.
- Investitionen in Cybersicherheit können dazu beitragen, Vorfälle unwahrscheinlicher zu machen, da die meisten Cyberkriminellen nach dem Weg des geringsten Widerstands suchen.



der Führungskräfte in Deutschland planen, in diesem Jahr Versicherungsoptionen zu prüfen – einschließlich Risiko- und Krisenmanagement.

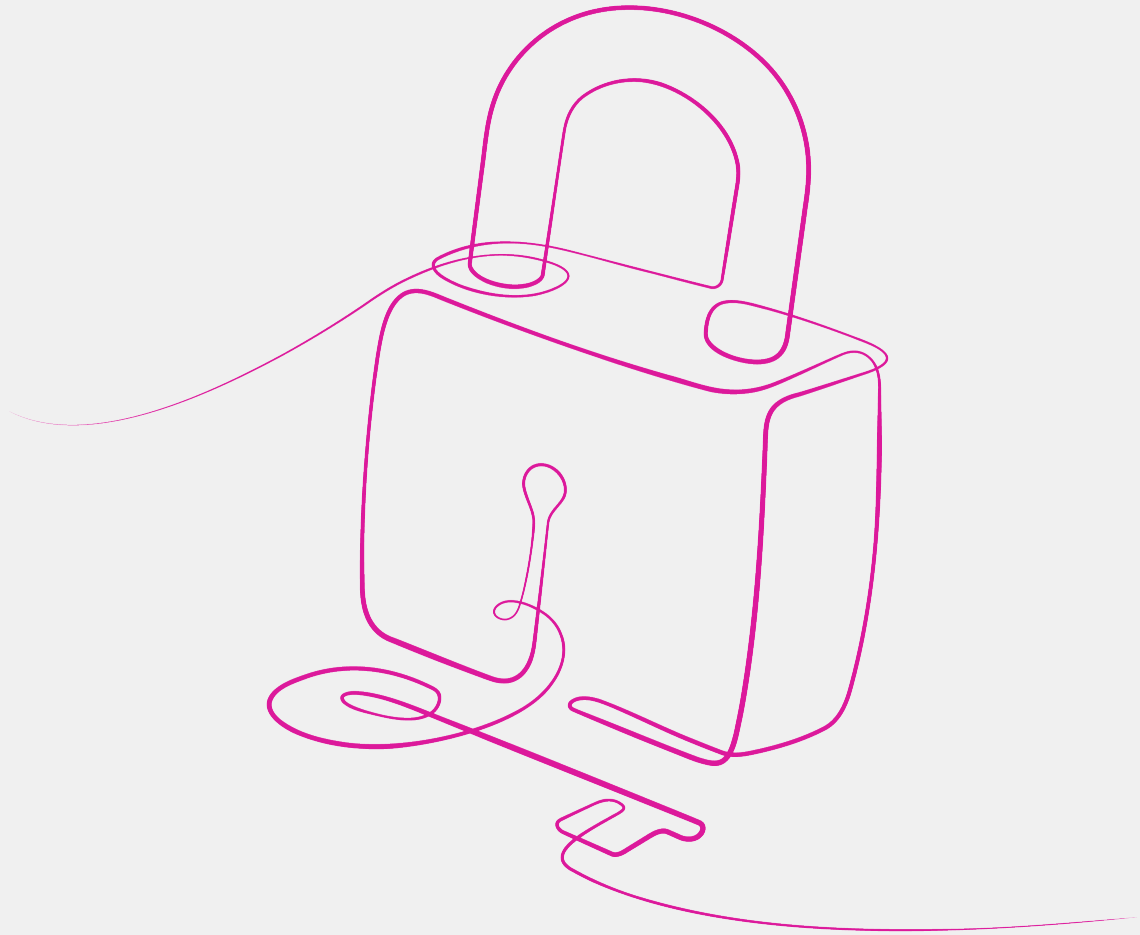


der in Deutschland ansässigen Führungskräfte geben an, dass ihr Vertrauen in den Wert von Versicherungen gestiegen ist.

beazley

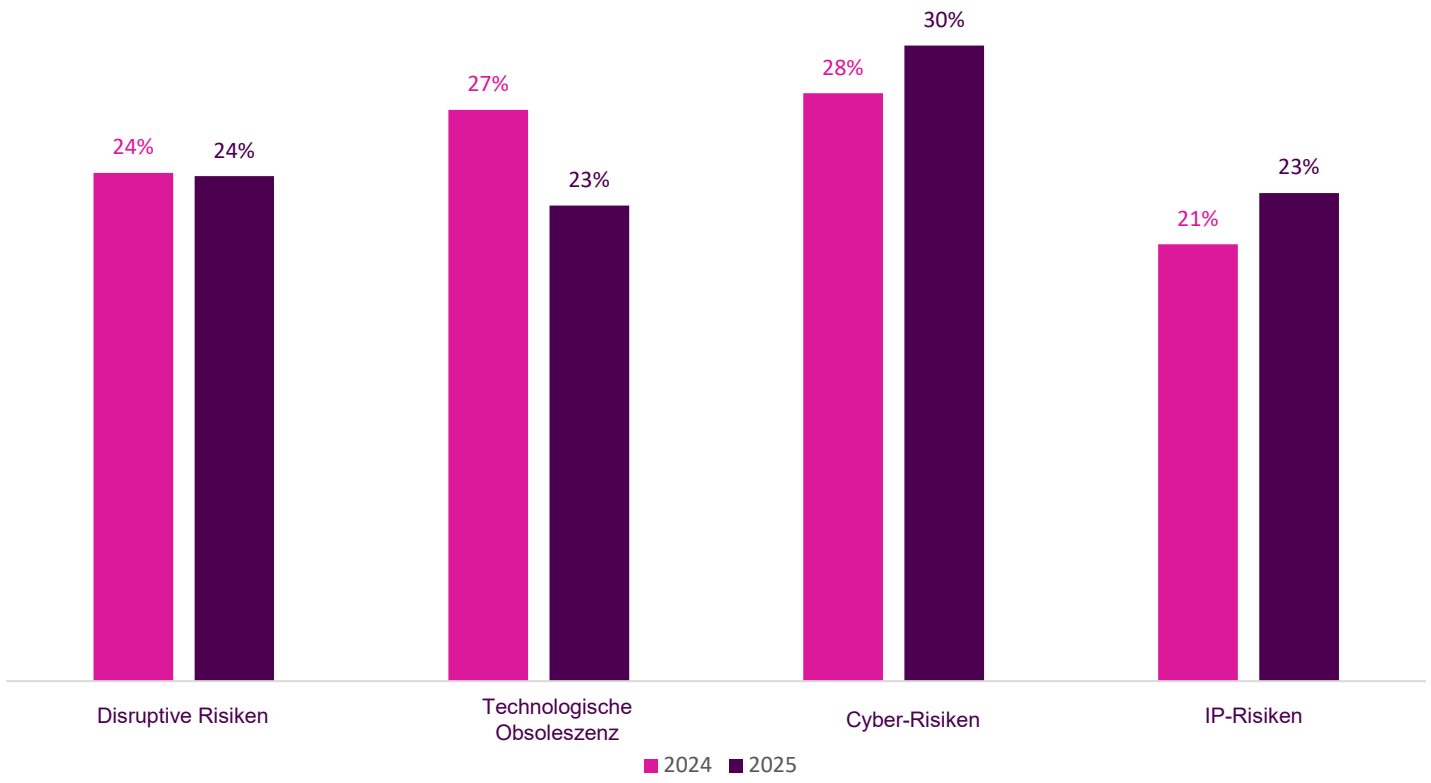
Risk & Resilience 2025

Datenübersicht



beazley

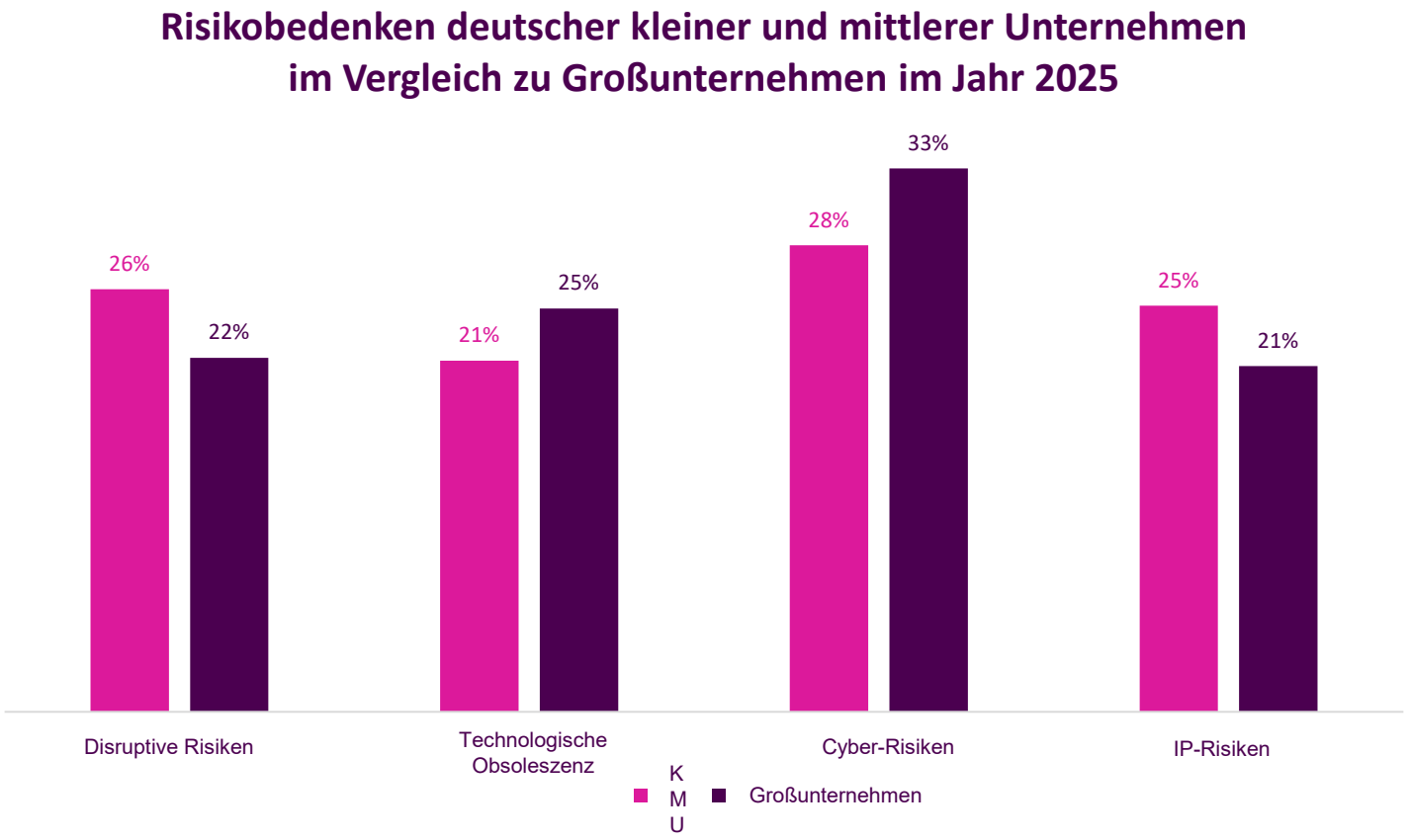
Deutschland: Cyber & Technology Risiko Ranking



Prozentsatz der Führungskräfte, die diese Risiken in den Jahren 2024 und 2025 als ihre größte Sorge einstufen.

beazley

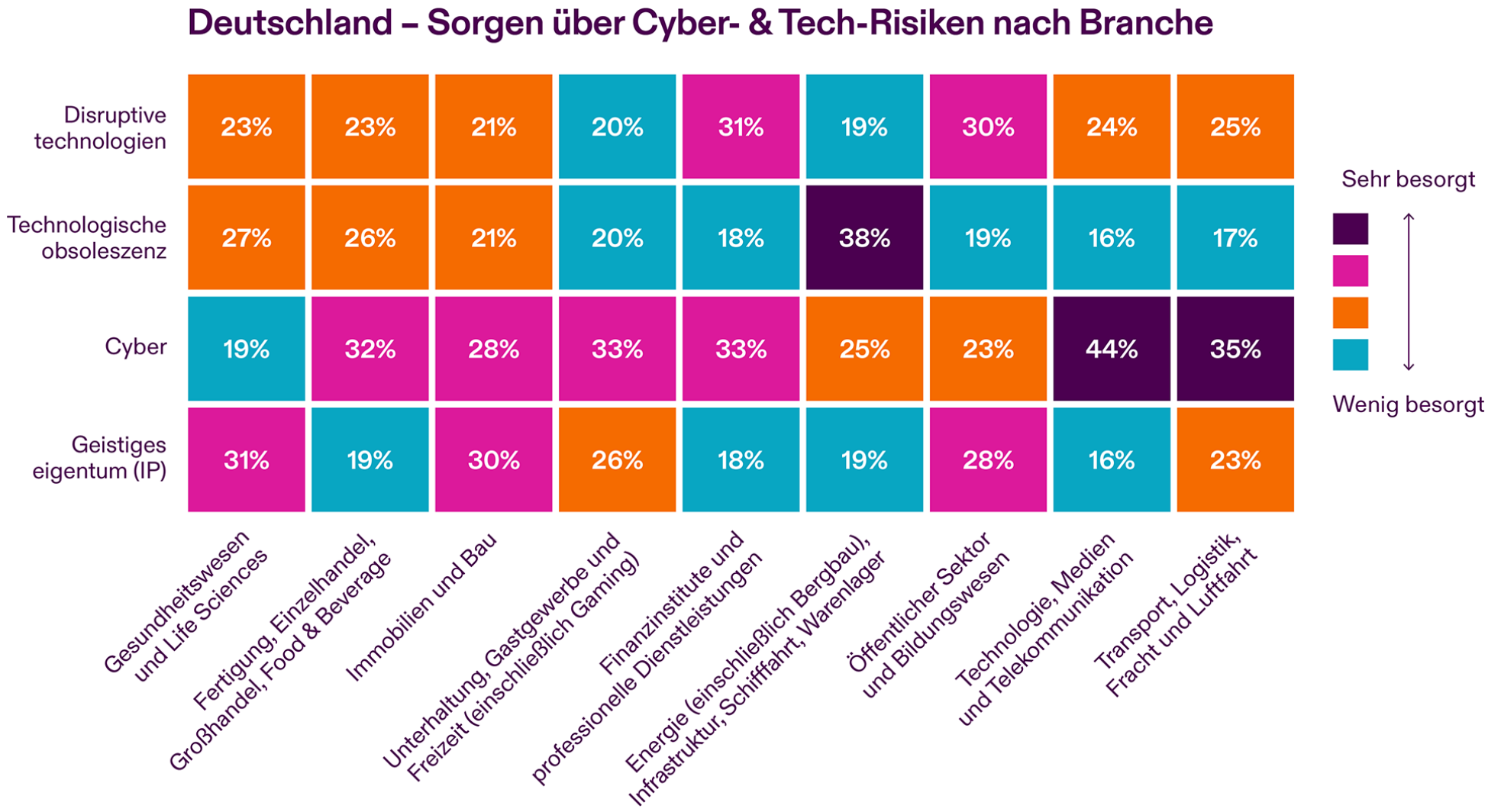
Deutschland: Cyber & Technology Risikobedenken



Prozentsatz der in Deutschland ansässigen Führungskräfte aus kleinen und mittleren Unternehmen (Jahresumsatz von 250.000 € bis 99,99 Mio. €) und Großunternehmen (ab 100 Mio. € Jahresumsatz), die bestimmte Risiken als ihre größte Sorge einstufen

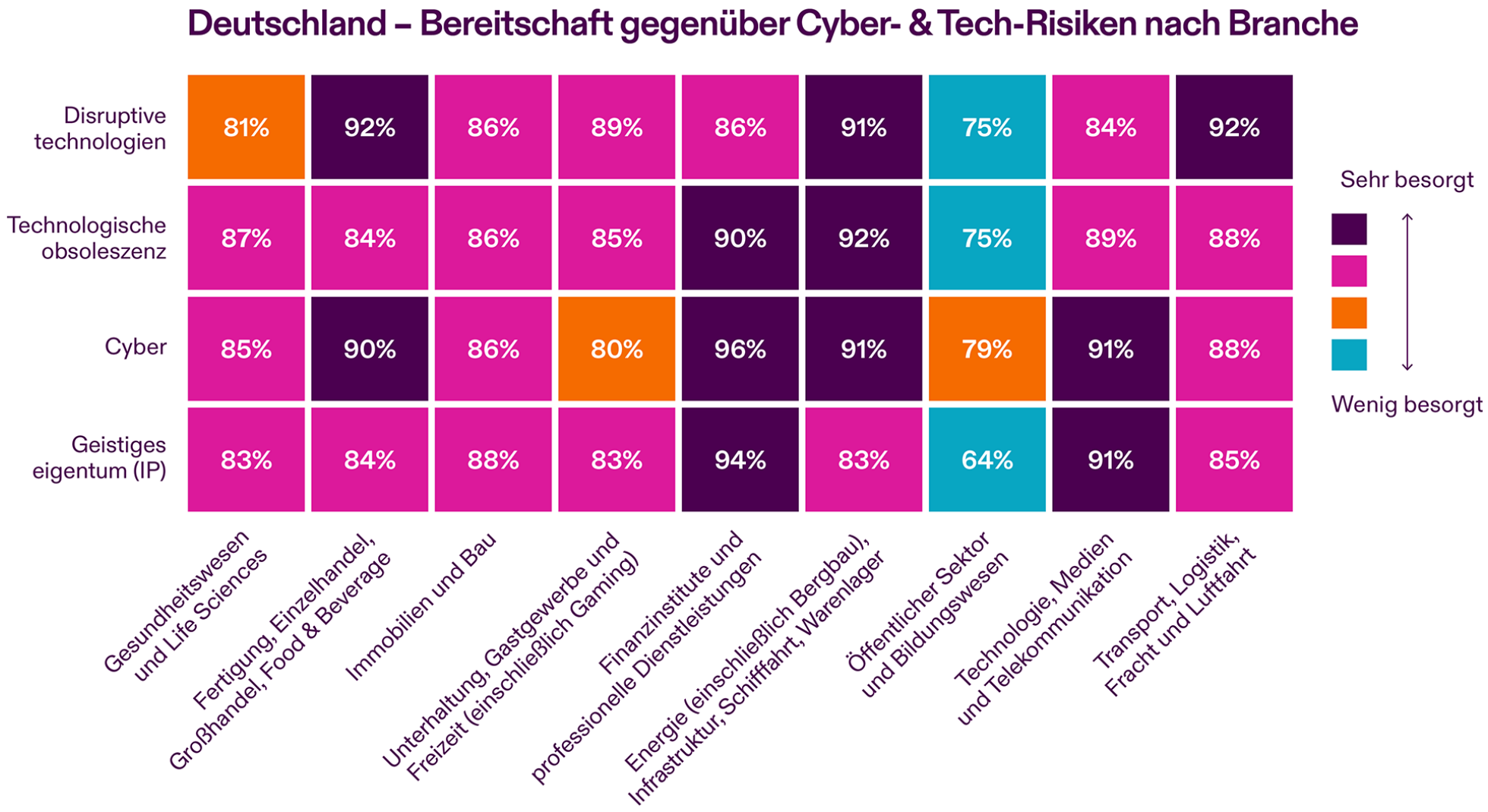
beazley

Globale Risiko Heatmap der Industrie



Der Prozentsatz der Führungskräfte, die diese Risiken in unserer Studie Risk & Resilience 2025/26 als ihr größtes Cyber- und Tech-Risiko eingestuft haben.

Globale Resilienz Heatmap der Industrie



Der Prozentsatz der Führungskräfte, die sich auf Cyber- & Tech-Risiken vorbereitet fühlen (Summe der Antworten ‚sehr gut vorbereitet' und ‚mäßig vorbereitet') laut unserer Studie Risk & Resilience 2025/26.

beazley

Beazley plc (BEZ.L) ist die Muttergesellschaft von Spezialversicherungsunternehmen mit Niederlassungen in Europa, den Vereinigten Staaten, Kanada, Lateinamerika und Asien. Beazley verwaltet sieben Lloyd's-Syndikate und zeichnete 2023 weltweit Bruttoprämien in Höhe von 6.164,1 Mio. USD. Alle Lloyd's-Syndikate werden von A.M. Best mit A bewertet.

Die Underwriter von Beazley in den Vereinigten Staaten konzentrieren sich auf die Erstellung einer Reihe von Spezialversicherungsprodukten. Auf dem zugelassenen Markt wird die Deckung von Beazley Insurance Company, Inc. bereitgestellt, einem von A.M. Best mit A bewerteten Versicherer, der in allen 50 Bundesstaaten zugelassen ist. Auf dem Markt für überschüssige Versicherungslinien wird die Deckung von Beazley Excess and Surplus Insurance, Inc. und den Beazley-Syndikaten bei Lloyd's bereitgestellt. Beazleys europäische Versicherungsgesellschaft, Beazley Insurance dac, wird von der irischen Zentralbank reguliert und hat ein A-Rating von A.M. Best und ein A+-Rating von Fitch.

Beazley ist Marktführer in vielen seiner ausgewählten Sparten, darunter Berufshaftpflicht, Cyber, Sach, Transport, Rückversicherung, Unfall und Leben sowie politische Risiken und Eventualgeschäfte.

Weitere Informationen finden Sie auf: beazley.com