Allianz



Hunyadi Marton / Shutterstock

ALLIANZ COMMERCIAL

# Business Black Swans

Survey: The threats companies consider to be most plausible in the next five years

commercial.allianz.com

OVERVIEW

# Interconnectivity and geopolitical instability raise fears of supply chain and cyber Black Swans

- → Supply chain paralysis and a global internet outage are seen as the two most plausible Black Swan scenarios in the next five years, according to a survey of more than 3,000 business and risk management experts.
- → Rare, high-impact events like these are perceived as being increasingly plausible in a world of interconnected supply chains, digital dependency, geopolitical volatility and trade wars.
- → Geopolitical noise masks risks from high impact climate, health and technology risks.
- → Organizational agility, resilience and integrated risk management are key to surviving Black Swan events, areas where companies are increasingly seeking external expertise and independent risk insights.

The scenarios discussed in this report are not considered to be immediately likely, but rather perceived to be plausible and possible in practice by survey respondents. While risk managers are naturally concerned with immediate and present risks, it is also valuable to think ahead about scenarios which could take place, albeit at lower probability, in order to scope out potential tail risks.

In an increasingly interconnected and volatile world, the likelihood of unforeseen, high-impact events – commonly referred to as Black Swans – is perceived to be rising sharply.

Historical examples such as the 2001 World Trade Center attacks, the 2008 global financial crisis, and the Covid-19 pandemic serve as stark reminders of their devastating impact. Allianz Research estimates that the cumulative global GDP losses from the pandemic alone amounted to approximately US$12trn between 2020 and 2023. In addition to the huge financial and business costs, such crises typically have long-lasting implications, resulting in geopolitical and societal shifts that continue many years after the initial event.

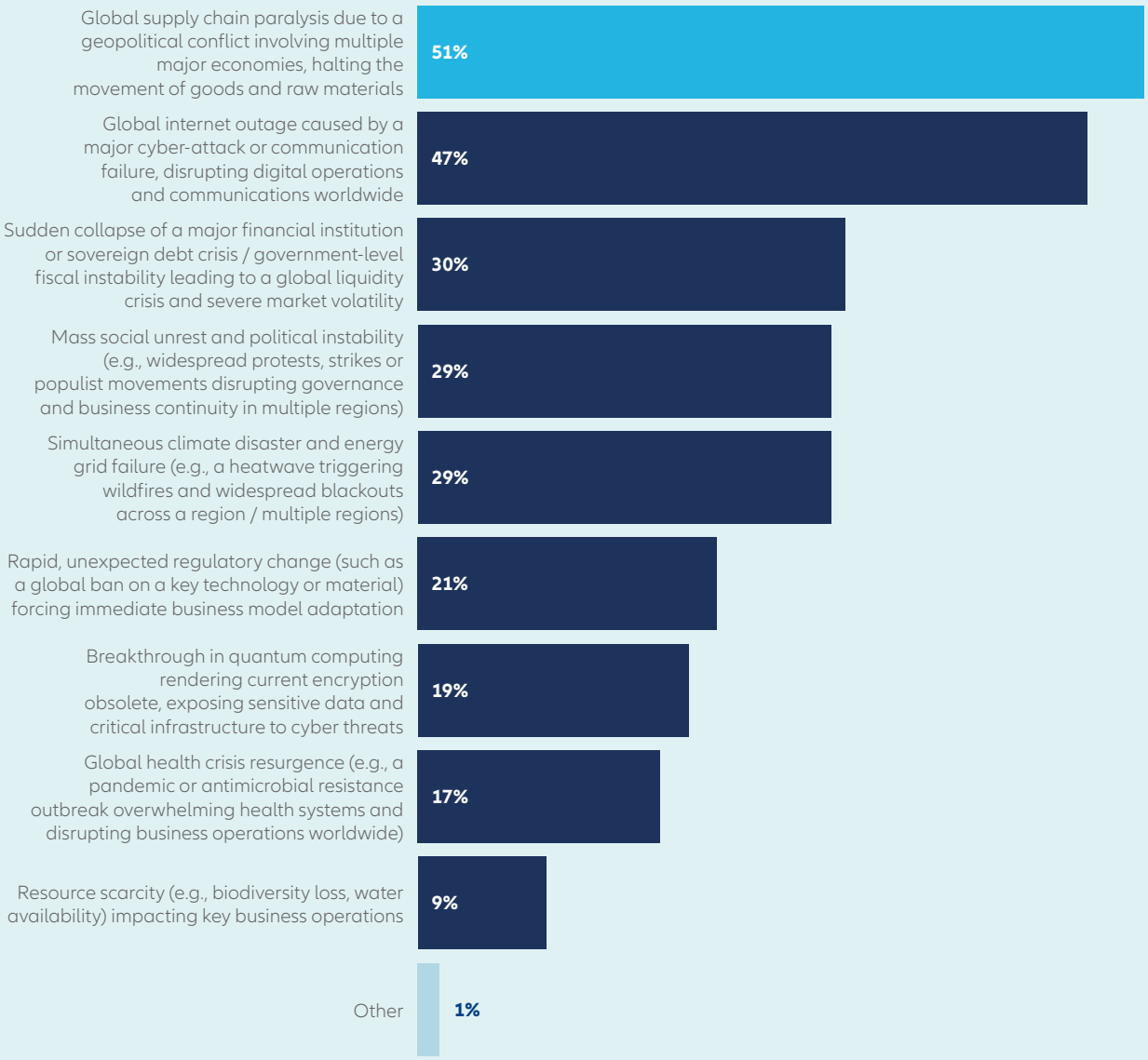
As physical and digital supply chains become ever more intertwined, disruptions can now propagate with unprecedented speed and scale. In today's fragmented geopolitical environment, resilience and proactive risk management are no longer optional – they are essential.

At Allianz Commercial, we recognize the critical importance of preparing for the next systemic shock and are committed to helping businesses and communities navigate these challenges. This report outlines potential scenarios that could arise, based on responses from risk management professionals globally. We hope that by sharing these insights, businesses are able to think far ahead, building resilience for the future by balancing the immediate with the long-term view and the likely with the unexpected.



**Thomas Lillelund**
CEO
Allianz Commercial

## **Global results:** Which of the following Black Swan scenarios do you consider most plausible for your company in the next five years?




**Over half of all respondents (51%)** believe that global supply chain paralysis resulting from a geopolitical conflict is the most plausible Black Swan scenario which could occur.

A global internet outage caused by a major cyber-attack or communication failure, disrupting operations worldwide **(47%) ranks second.**

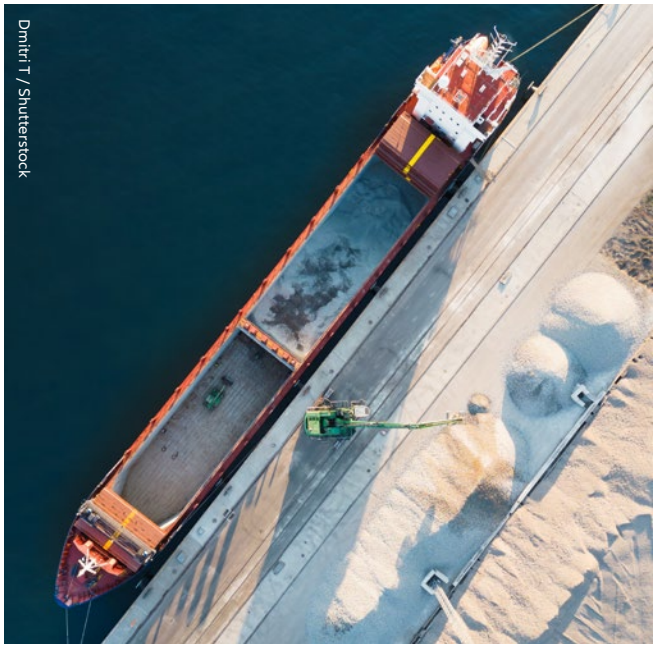
The sudden collapse of a major financial institution or a sovereign debt crisis is **third (30%).**

Number of respondents: 3,338. Respondents could select up to three scenarios.
Source: Allianz Risk Barometer 2026.

# Supply chain paralysis and global outages rank as the most feared Black Swan events

Global supply chain paralysis due to a geopolitical conflict halting the movement of goods and raw materials is considered the most plausible Black Swan scenario globally in the next five years (51% of responses), according to new **Allianz Risk Barometer** analysis, which surveyed 3,338 risk management experts from almost 100 countries and territories.

This scenario is perceived as being the most plausible Black Swan event by European (57%) and Asia Pacific (48%) respondents, and by those in the US (52%) and China (51%), for example. It ranks even higher in export-led Germany (71%). It is also seen as the leading scenario by large companies (>US$500mn annual revenue) and by most sectors, including manufacturing, transport, heavy industry, retail, food, and consumer goods.


Dmitri T / Shutterstock

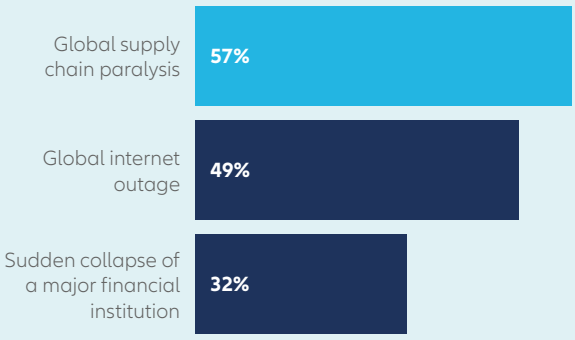
A global internet outage caused by a major cyber-attack or technology failure, disrupting digital operations and communications worldwide, is regarded as the second most plausible Black Swan scenario globally (47%). It is the most feared event for respondents in the Americas (49%) and Africa and Middle East (51%) regions, as well as in the UK (69%), Brazil (48%), Colombia (55%), India (42%) and Australia (45%), for example. Global internet outage also ranks top according to respondents from smaller companies (<US$100mn annual revenue) and those from the financial services, professional services, government, technology, telecoms, media, entertainment, and hospitality sectors.

Supply chain paralysis and global internet outages are front of mind for many businesses, reflecting the critical nature of global supply chains and digitalization in an increasingly volatile geopolitical climate. They are also the scenarios that are likely to manifest sooner than other plausible scenarios, such as a climate, health, or technology-related global crisis, which are seen as more distant and longer-term by respondents.

*"The unpredictable geopolitical landscape and persistence of cyber-attacks and outages are factors in respondents perceiving that the supply chain paralysis and internet outage scenarios are more likely to occur sooner than others,"* says **Michael Bruch, Global Head of Risk Consulting Advisory Services, Allianz Commercial.** *"Despite progress in cyber and supply chain resilience threats continue to evolve. Many organizations still lack sufficient visibility into the dependencies and vulnerabilities embedded in their physical and digital supply chains. Understanding these linkages is the foundation of resilience. Yet their growing opacity is often underestimated."*

## **Region:** Europe

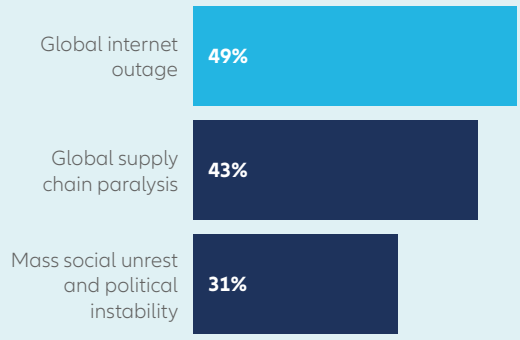
### Top 3 responses




Number of respondents: 1,599.

## **Region:** Americas

### Top 3 responses

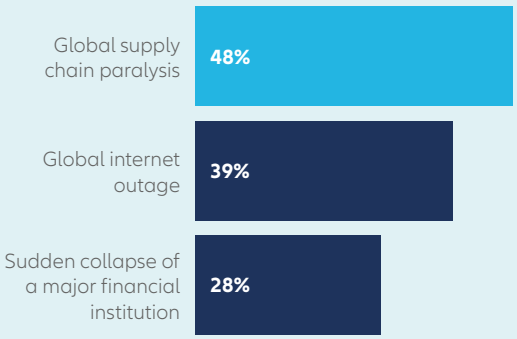



Number of respondents: 832.

**Global internet outage**, and **mass social unrest and political instability** rank higher in the Americas region than globally.

## **Region:** Asia Pacific

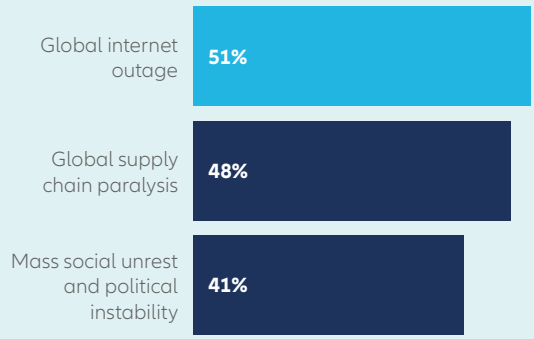
### Top 3 responses




Number of respondents: 823

## **Region:** Africa and Middle East

### Top 3 responses




Number of respondents: 84.

**Global internet outage**, and **mass social unrest and political instability** rank higher in the Africa and Middle East region than globally.

Respondents could select up to three scenarios.
Source: Allianz Risk Barometer 2026.
Statements highlight where regional results differ from the global results.

# Geopolitics is a key driver for Black Swans

It is little surprise that supply chain paralysis resulting from a geopolitical conflict is regarded as the most plausible Black Swan scenario, given the threats of tariffs, trade wars and protectionism, as well as disruption to supply chains and shipping caused by regional conflicts in the Middle East and Russia/Ukraine. **Allianz Research** estimates that cumulative GDP losses over a two-year horizon triggered by a global supply chain disruption on the scale of the war in Ukraine could total US$1.5trn.

In fact, political-related risks stand out as a leading potential trigger for Black Swan events, according to respondents. Mass social unrest and political instability is regarded as the fourth most plausible scenario globally (29%) and is a top three risk in the Americas (31%) and Africa and the Middle East (41%) regions, as well as in France (42%), for example.

*"Global geopolitical instability, combined with persistent political violence and escalating SRCC (strike, riot, and civil commotion) activities worldwide, underscores the necessity for businesses to remain vigilant regarding the dynamic nature of such risks,"* says **Kostas Papapetridis, Regional Head of Risk Consulting, North America, Allianz Commercial.**

*"The interplay between political and social polarization, environmental challenges, and economic uncertainty is increasingly manifesting in civil unrest across diverse regions. These disturbances often escalate into protests characterized by threats, unpredictability, and violence. As we look to the future, it is expected that protest movements, irrespective of geographical boundaries and economic conditions, will continue to rise, posing significant challenges for global supply chains and necessitating robust risk management strategies that take into account the global scenery of SRCCs."*

Similarly, rapid, unexpected regulatory change, such as a global ban on a key technology or material, ranks as the sixth most plausible Black Swan scenario of concern (21%) globally, and is a top three concern for respondents in China (35%) and Singapore (32%).

Increasingly, nation states are exploiting supply chain vulnerabilities and dependencies on undiversified sources of raw materials, critical products and services. In 2025, China tightened export controls on rare earth elements amid an on-off trade dispute with the US. There are also fears that a future rise in tensions between the US and China in the Pacific, which could involve a potential blockade of Taiwan, could disrupt shipping in the region and the supply of critical components like semiconductors. Bloomberg[1] has estimated the potential impact of such a scenario on the global economy could be as high as US$5trn.

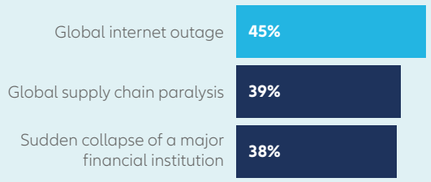


Sergey Nivens / Shutterstock

## Selected countries

### Top 3 responses

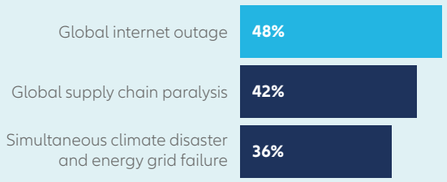
#### Australia




**Global internet outage** ranks as the most plausible scenario.

Number of respondents: 88.

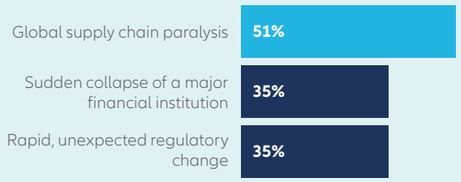
#### Brazil




**Global internet outage** is the most plausible scenario, while **simultaneous climate disaster and energy grid failure** ranks higher in Brazil than globally.

Number of respondents: 131.

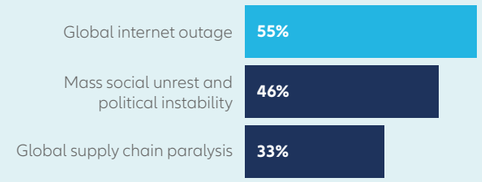
#### China




**Sudden collapse of a major financial institution or sovereign debt crisis**, and **rapid unexpected regulatory change** rank higher in China than globally.

Number of respondents: 192.

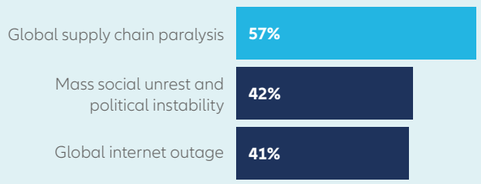
#### Colombia




**Global internet outage**, and **mass social unrest and political instability** rank higher in Colombia than globally.

Number of respondents: 226.

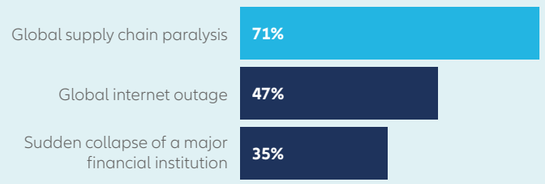
#### France




**Mass social unrest and political instability** ranks higher in France than globally.

Number of respondents: 150.

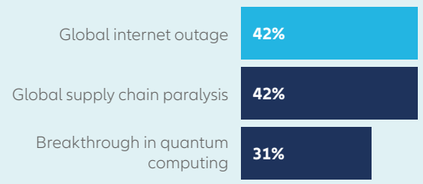
#### Germany




German respondents rank **global supply chain paralysis** much higher than respondents globally.

Number of respondents: 400.

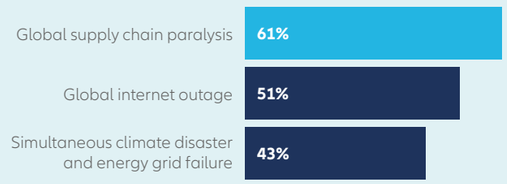
#### India




**Global internet outage** and a **breakthrough in quantum computing rendering current encryption obsolete** rank higher in India than globally.

Number of respondents: 98.

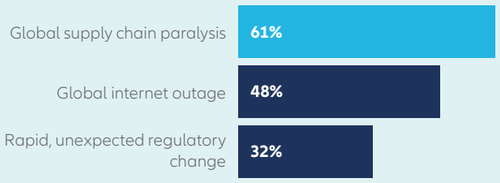
#### Italy




**Simultaneous climate disaster and energy grid failure** ranks higher in Italy than globally.

Number of respondents: 168.

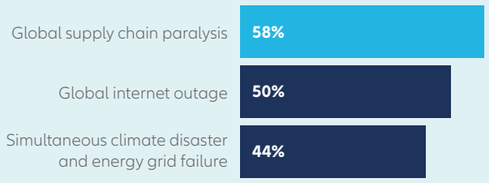
#### Singapore




**Rapid, unexpected regulatory change** ranks higher in Singapore than globally.

Number of respondents: 120.

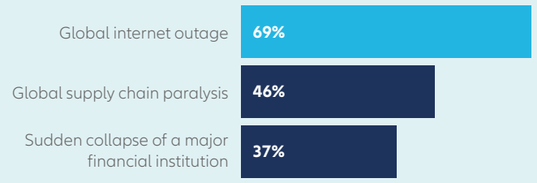
#### Spain




**Simultaneous climate disaster** and **energy grid failure** ranks higher in Spain than globally.

Number of respondents: 102.

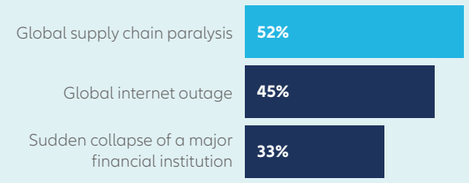
#### UK




**Global internet outage** ranks higher in the UK than globally.

Number of respondents: 131.

#### US




Number of respondents: 262.

Respondents could select up to three scenarios.
Source: Allianz Risk Barometer 2026.
Statements highlight where country results differ from the global results.

**For more country results, see page 17**

# Digital dependencies raise concerns about global internet outage

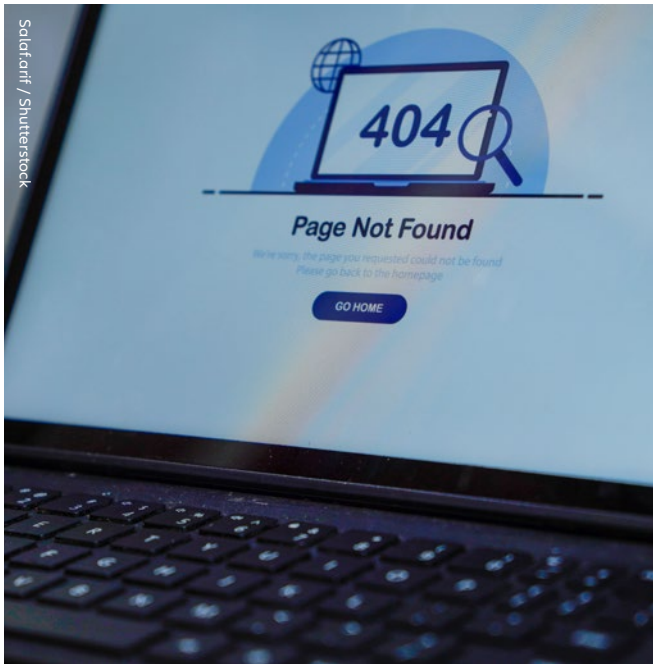
Concern about a global internet outage reflects the growing awareness of cyber risk and digital interdependency, which has accelerated since the Covid-19 pandemic. Recent years have seen a number of near misses – a flawed update of CrowdStrike software in 2024 affected millions of systems running Windows, while a system error at internet infrastructure provider AWS in October 2025 caused a widespread internet outage, affecting over 1,000 companies[2] and millions of internet users. Costs from the CrowdStrike event alone have been estimated as being as high as billions of dollars[3].

A global internet outage could arise from multiple scenarios, including a malicious cyber-attack or technical failure affecting a critical infrastructure or service provider, or the consequence of an external event, such as extreme weather or a solar storm – in 2025, Lloyd's[4] estimated the global economy could be exposed to losses of US$2.4trn over a five-year period from a hypothetical solar storm, while two years earlier it estimated a major global cyber-attack could trigger a US$3.5trn[5] loss over a five-year period.

Tech company Cloudflare[6] tracked over 180 internet disruptions worldwide in 2025. Some lasted several days, resulting from a wide range of causes, including power outages, subsea communications cable damage, as well as technical glitches.

The risk of a global outage could also increase with the growing reliance on a small number of technology companies, according to **Michael Bruch, Global Head of Risk Consulting Advisory Services, Allianz Commercial:** *"We are facing a new kind of 'monopoly risk' as critical digital infrastructure becomes concentrated among a small number of providers. A single point of failure – whether technical or cyber-related – could trigger global repercussions. Building resilience against these systemic exposures should be a priority for every organization."*

> We are facing a new kind of 'monopoly risk' as critical digital infrastructure becomes concentrated among a small number of providers



Solafarif / Shutterstock

# Vulnerable grid infrastructure raises risk of prolonged power outage

The growing dependency on electrical power grids and digital technology is particularly concerning given the energy transition, climate change and ageing infrastructure, according to **Daniel Muller, Head of Emerging Risks and Trends, Allianz Commercial.** Simultaneous climate disaster and energy grid failure (29% of responses) ranks fifth as the most plausible Black Swan globally and is notably of high concern in Italy (43%), Spain (44%) and Brazil (36%). Interestingly, it is viewed as a top three risk by large companies (>US$500mn annual revenue), (33%) and is seen as the biggest Black Swan risk by respondents in the power and renewables sector.

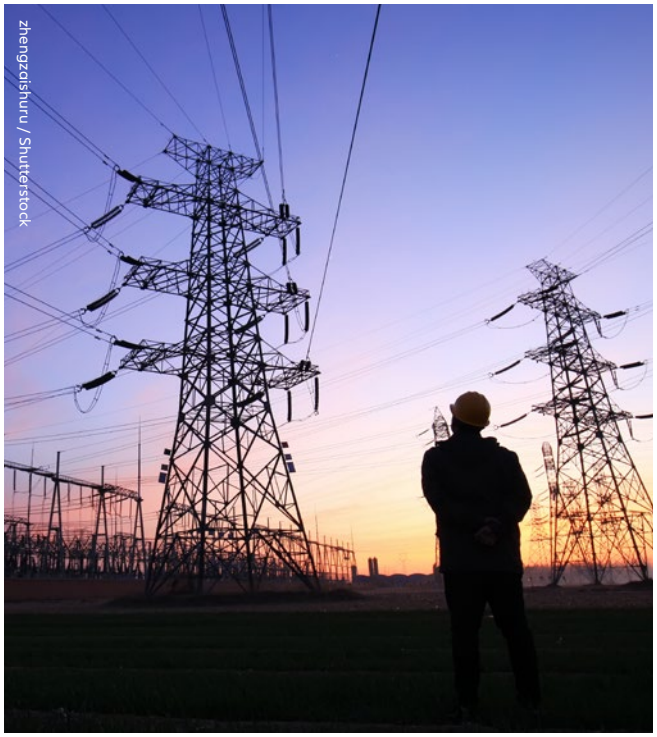
*"Climate change combined with ageing critical infrastructure is creating a growing systemic vulnerability. Extreme temperatures and weather events are increasingly pushing grids beyond their design limits, and when these systems fail, the resulting power outages can trigger cascading disruptions across digital services, transport, industrial operations, and financial systems,"* says **Muller.**

A large power surge is believed to have contributed to a day-long blackout in Spain and Portugal last year, the most severe in Europe for over 20 years. The outage, which also damaged industrial plant, equipment and stock, is estimated to have cost the Spanish economy as much as US$1.8bn[7]. In January 2026, an arson attack in Germany resulted in several days of blackouts in parts of Berlin, while a fire at a substation shut down London's Heathrow airport in March 2025.

High levels of dependency and interconnectivity could make such events more likely and have a higher impact than in the past, according to **Muller:**

*"Data centers and artificial intelligence (AI) infrastructure are increasingly becoming the backbone of modern economies, but they are only as resilient as the power grids that support them. With electricity demand accelerating and much of the world's infrastructure now decades old, the likelihood of prolonged outages – and their far-reaching ripple effects – is rising quickly."*

> Data centers and artificial intelligence (AI) infrastructure are becoming the backbone of modern economies, but they are only as resilient as the power grids that support them



zhengzaishuru / Shutterstock

# Financial market turbulence potential

Despite ongoing geopolitical instability and the implementation of sweeping US tariffs, the global economy has proven resilient to date. Having performed better than expected in 2025, **Allianz Research** expects global GDP to grow 2.9% in 2026. Yet, even as the global economy shows impressive resilience, the operating environment is becoming more volatile, more fragmented, and more strategically contested.

According to respondents, the sudden collapse of a major financial institution or sovereign debt crisis is the third most plausible Black Swan scenario that could occur within the next five years (30%). It ranks second in China (35%) and is a high concern for respondents in Australia (38%), UK (37%), Germany (35%) and the US (33%).

The potential scenario worries smaller (<US$100mn annual revenue) and mid-sized (US$100mn+ to US$500mn annual revenue) companies, which rank it as the third most plausible, higher than large firms (>US$500mn annual revenue).

Potential triggers for financial market turbulence include geopolitical risks, crises in sovereign debt and / or private credit markets, and a possible AI-equity correction, according to respondents. In its January 2026 economic outlook, the International Monetary Fund (IMF)[8] warned that the bursting of an AI-equity bubble and / or intensifying trade tensions could impact financial markets and household wealth, and disrupt the global economy.



ST House Studio / Shutterstock

# Distant risks are underappreciated

More distant seeming Black Swan scenarios, such as a major health or climate crisis, or a sudden advancement in a disruptive technology, are seen as less plausible in the next five years, according to respondents.

A breakthrough in quantum computing rendering current encryption obsolete, exposing sensitive data and critical infrastructure to cyber threats ranks seventh (19%) globally, although it ranks third in India (31%). This is followed by a global health crisis, such as a pandemic or antimicrobial resistance outbreak (17%), and resource scarcity, such as biodiversity loss and water availability (9%).

These scenarios, while considered plausible within the five-year timeframe by some, are seen as longer-term future threats. Quantum computing, for example, is not expected to reach commercial viability for another five to 10 years. However, the technology has made surprising advancements in recent years, and a major breakthrough could give rise to entirely new forms of cyber-attacks and undermine today's encryption standards.

Climate tipping points – such as the collapse of the Gulf Stream and thawing of the polar ice sheets or permafrost – is another high impact scenario that is perceived as longer term. According to the Intergovernmental Panel on Climate Change (IPCC) the likelihood and impacts[9] of abrupt and / or irreversible changes in the climate system increase with global warming. Shortages of natural resources, such as water, could also have wide-ranging implications for supply chains, transport and geopolitics.

*"It's difficult to cut through all the noise today and take in the long-term risks. Climate change and biodiversity loss remain key risks longer-term, yet they are often underestimated amid geopolitical risks like tariffs and regional conflicts. Climate change risks will not disappear because attention shifts elsewhere. Companies must embed long-term resilience thinking alongside short-term geopolitical risk management,"* says **Michael Bruch, Global Head of Risk Consulting Advisory Services, Allianz Commercial.**

> Climate change risks will not disappear because attention shifts elsewhere


Bernhard Staehli / Shutterstock

# Interconnectivity is driving heightened risk of Black Swans

Interconnectivity and interdependency of both physical and digital supply chains are potentially increasing vulnerability at a time of geopolitical uncertainty, rapid advances in technology and climate change. Businesses and global supply chains are also more vulnerable to Black Swan events due to growing concentrations of economic activity on a limited numbers of critical suppliers of products and suppliers in areas like artificial intelligence (AI) and digital services, semiconductors, rare earth processors and transition technologies.

*"The growing concentration of critical products and technologies among a limited number of suppliers creates significant systemic exposure. If one of these providers suffers a cyber-attack, a trade restriction, or operational failure, the disruption can rapidly cascade across global physical and digital supply chains. Some essential components – such as power transformers – can take as long as three to five years to replace, amplifying the potential scale of business interruption,"* says **Daniel Muller, Head of Emerging Risks and Trends, Allianz Commercial.**

There is also the potential for multiple Black Swan events to occur simultaneously, or in succession. Many Black Swans are themselves interconnected, with one event potentially giving rise to another. For example, a solar storm could result in a long-lasting widespread power and communications blackout, triggering economic and financial market volatility and social unrest. Similarly, a large-scale nation-state cyber-attack could target critical suppliers, infrastructure and / or financial institutions.

*"The survey highlights how deeply interconnected today's global economy has become. A single Black Swan event can trigger cascading effects across businesses, financial markets and economies around the world. Digitalization continues to intensify these interdependencies,"* says **Michael Bruch, Global Head of Risk Consulting Advisory Services, Allianz Commercial.**

> The concentration of critical products and technologies within a handful of suppliers creates systemic exposure



Michael Vi / Shutterstock

# Survey findings highlight need for resilience, agility and integrated risk management

In a world where the potential for Black Swan events is becoming more frequent and impactful, companies will need to be resilient. A recent study[10] by the World Economic Forum found that almost three in four business leaders now prioritize resilience investments, with 74% viewing resilience as a driver of growth.

Business interruption and supply chain disruption ranks as the third most concerning business risk globally in the **Allianz Risk Barometer,** just behind artificial intelligence (AI) and cyber. Yet just 3% of respondents view their supply chains as "very resilient". According to respondents, the top actions companies are taking to address the impact of shifting trade policies and tariffs is to explore new markets and products, as well as looking at renegotiating and diversifying supply chains.

*"Awareness of Black Swans and the need to build resilience has increased in recent years, but businesses can never fully prepare for rare high impact events such as a global outage or an unforeseen climate-related catastrophe. It's always a balancing act between investment in resilience and day-to-day business needs. And this balance is not easy to achieve, especially for smaller companies that do not have the expertise to do that,"* says **Michael Bruch, Global Head of Risk Consulting Advisory Services, Allianz Commercial.**

As risk becomes more complex and interconnected, integrated resilience strategies can help to mitigate the impact. Companies now need to have forward-looking approaches to managing risk, including dynamic horizon scanning, scenario modelling, and rigorous stress testing. An integrated resilience strategy can also help avoid unintended consequences as companies adapt their operations and supply chains in response to geopolitical risks and sustainability concerns.

*"Preparing for Black Swans demands a coordinated, enterprise-wide approach – no single function can manage such systemic shocks on its own. The survey highlights the importance of building truly cross-functional resilience. These events rarely remain confined to one part of the business – they ripple across finance, operations, IT, and supply chains,"* says **Daniel Muller, Head of Emerging Risks and Trends, Allianz Commercial.**

*"Preparing for a Black Swan risk involves bracing for the improbable possibility, necessitating a deep comprehension of the intricate web of interconnected risks, the probabilistic nature of modeling tools, and a touch of imaginative foresight,"* adds **Kostas Papapetridis, Regional Head of Risk Consulting, North America, Allianz Commercial.**

*"The future risk environment will continue to evolve, and the organizations best prepared are those that continuously assess, adapt, and embed resilience at every level of their operations."*

Being more flexible will help companies respond quickly to rare, high-impact events, says **Bruch:**

*"Building organizational agility, fostering a risk-aware culture and developing scalable response plans for a range of scenarios remain the most practical steps to prepare for Black Swan events. Diverse expertise and perspectives are essential in scenario planning. It's not rocket science, but it is challenging to execute consistently.*

*"Risk management cannot sit in a single function – every employee needs to adopt a risk mindset. Identifying risks, evaluating them, mitigating them, and recognizing opportunities arising from disruption should be part of everyday decision-making."*

## Differences between large and small companies

### Large companies (>US$500mn annual revenue)
Top 3 responses




Number of respondents: 1,471.

### Mid-sized companies (US$100mn+ to US$500mn annual revenue)
Top 3 responses




Number of respondents: 816.

### Smaller companies (<US$100mn annual revenue)
Top 3 responses




Number of respondents: 1,051.

Respondents could select up to three scenarios.
Source: Allianz Risk Barometer 2026.

Global supply chain paralysis due to a geopolitical conflict halting the movement of goods and raw materials ranks top for both large (55% of responses) and mid-sized companies (52%). In contrast, smaller companies are most concerned about the impact of a global internet outage (45%).

While companies of all sizes are worried about global supply chain paralysis (ranked second by smaller companies), mid-sized and smaller companies rank the sudden collapse of a major financial institution or a sovereign debt crisis, for example, as the third most plausible scenario, while larger companies are more concerned about the risk of simultaneous climate disaster and energy grid failure.

Large and mid-sized companies are likely less concerned with the risk of internet outages than smaller companies because they are more diversified and have their own IT and cyber security departments, explains **Daniel Muller, Head of Emerging Risks and Trends, Allianz Commercial:**

*"Smaller companies often find it difficult to invest in resilience to the same extent as larger organizations, because they lack dedicated resources and specialized expertise in areas such as cyber security and supply chain management. As a result, they remain more vulnerable to prolonged digital or operational disruptions. Insurers can play a critical role by helping these businesses strengthen their cyber resilience and make more informed decisions when assessing and selecting critical suppliers."*

*"Insurers are not just about risk transfer providers, they are resilience partners,"* says **Michael Bruch, Global Head of Risk Consulting Advisory Services, Allianz Commercial.** *"Insurers support clients with independent risk insights and practical resilience services. Investing in resilience helps businesses to withstand high-impact events and recover faster – and even seize the opportunities that follow."*

## Most plausible Black Swan scenarios by selected industry sectors

**AGRICULTURE**
Global supply chain paralysis

**AVIATION**
Global supply chain paralysis

**CHEMICALS**
Global supply chain paralysis

**CONSUMER GOODS**
Global supply chain paralysis

**ENGINEERING**
Global supply chain paralysis

**ENTERTAINMENT**
Global internet outage

**FINANCIAL SERVICES**
Global internet outage

**FOOD**
Global supply chain paralysis

**GOVERNMENT**
Global internet outage

**HOSPITALITY**
Global internet outage

**MANUFACTURING (AUTOMOTIVE)**
Global supply chain paralysis

**MANUFACTURING (OTHER)**
Global supply chain paralysis

**MARINE**
Global supply chain paralysis

**MEDIA**
Global internet outage

**MINING**
Global supply chain paralysis

**OIL AND GAS**
Global supply chain paralysis

**POWER AND UTILITIES**
Simultaneous climate disaster and energy grid failure

**PROFESSIONAL SERVICES**
Global internet outage

**RENEWABLE ENERGY**
Simultaneous climate disaster and energy grid failure

**RETAIL**
Global supply chain paralysis

**TECHNOLOGY**
Global internet outage

**TELECOMMUNICATIONS**
Global internet outage

**TRANSPORTATION**
Global supply chain paralysis

Number of respondents: 3,338.
Respondents could select up to three scenarios.
Source: Allianz Risk Barometer 2026.

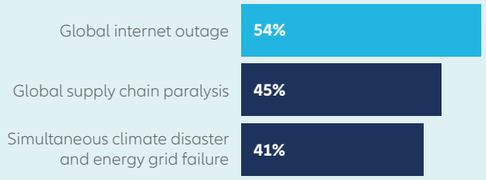
# References


1 Bloomberg, China 'Blockade Simulation' Exposes $5 Trillion Global Danger, May 5, 2024
2 Yahoo News, Which sites and apps were hit by the mass AWS internet outage?, October 20, 2025
3 Parametrix, CrowdStrike to Cost Fortune 500 $5.4b; Insured Loss Range of $0.54b – $1.08b, July 24, 2024
4 Lloyd's, Lloyd's highlights risk of extreme space weather as latest scenario reveals potential global economic loss of $2.4trn, March 4, 2025
5 Lloyd's, Lloyd's systemic risk scenario reveals global economy exposed to $3.5trn from major cyber attack
6 Cloudfare, Cable cuts, storms, and DNS: a look at Internet disruptions in Q4 2025, January 26, 2026
7 Reuters, Post-blackout in Spain and Portugal, companies count the cost, April 29, 2025
8 International Monetary Fund, World Economic Outlook Update, January 2026
9 UK Met Office, What do we mean by a climate tipping point? September 7, 2023
10 World Economic Forum, Global supply chains enter era of structural volatility, World Economic Forum report finds, January 19, 2026

# **Results appendix:** Additional countries and territories

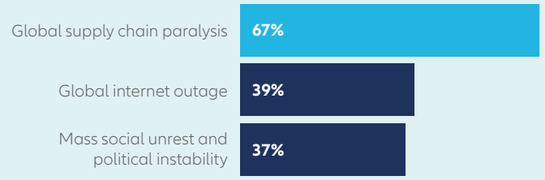
## Top 3 responses

### Argentina



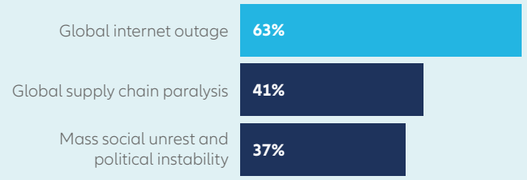

Number of respondents: 76.

### Austria



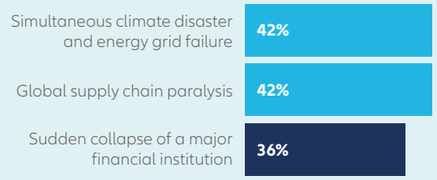

Number of respondents: 57.

### Belgium



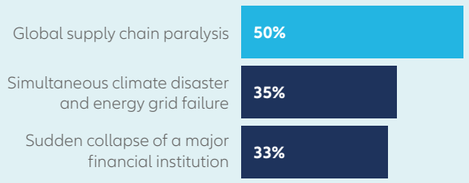

Number of respondents: 27.

### Bulgaria



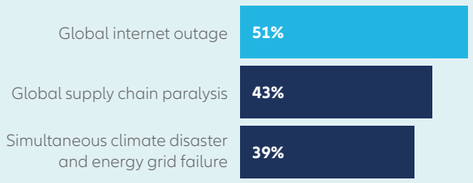

Number of respondents: 33.

### Canada



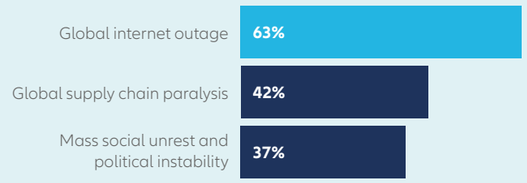

Number of respondents: 54.

### Croatia



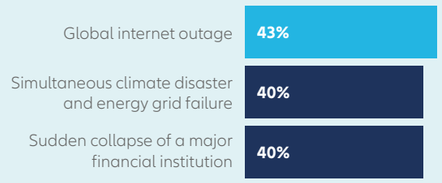

Number of respondents: 49.

### Czech Republic



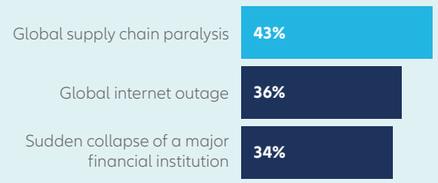

Number of respondents: 19.

### Greece



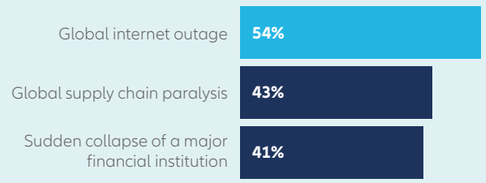

Number of respondents: 40.

### Hong Kong



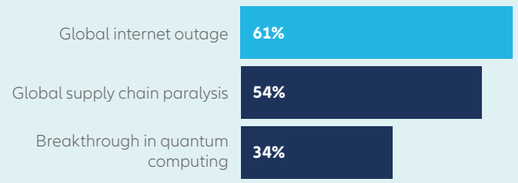

Number of respondents: 47.

### Hungary



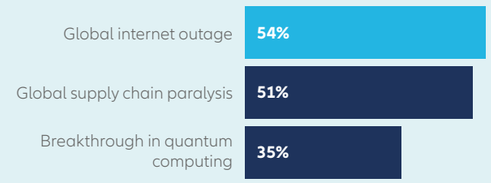

Number of respondents: 46.

### Japan




Number of respondents: 59.

### Malaysia



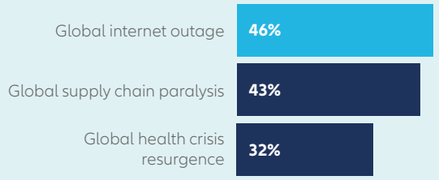

Number of respondents: 37.

Respondents could select up to three scenarios.
Source: Allianz Risk Barometer 2026.

# **Results appendix:** Additional countries and territories

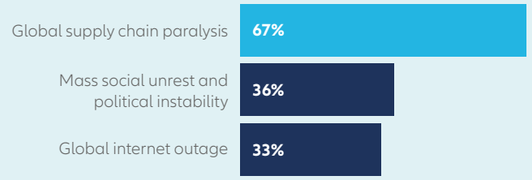
## Top 3 responses

### Mexico



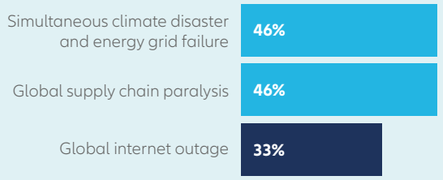

Number of respondents: 63.

### Netherlands



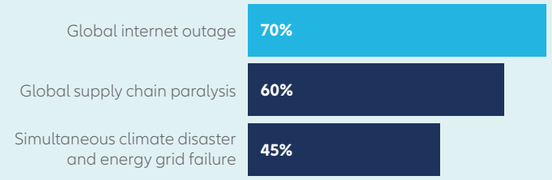

Number of respondents: 36.

### Philippines



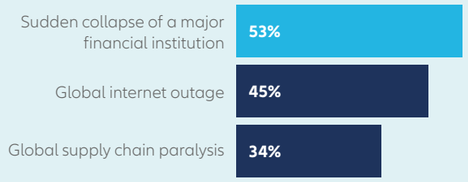

Number of respondents: 24.

### Portugal



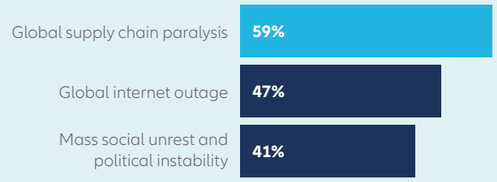

Number of respondents: 77.

### Romania



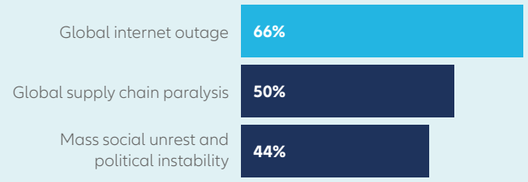

Number of respondents: 92.

### Slovenia



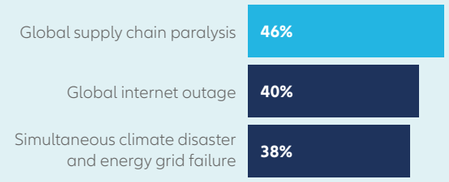

Number of respondents: 17.

### South Africa



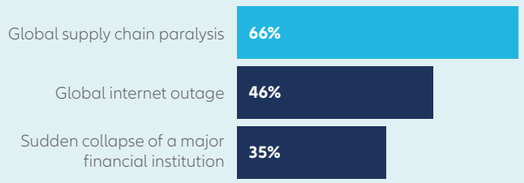

Number of respondents: 50.

### South Korea



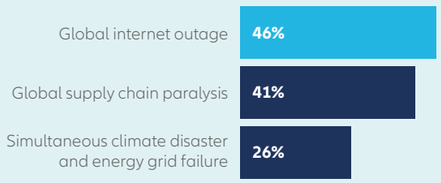

Number of respondents: 80.

### Switzerland



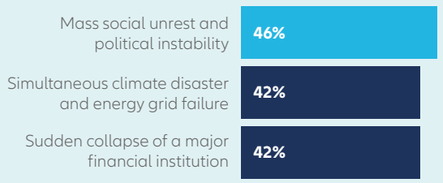

Number of respondents: 65.

### Thailand




Number of respondents: 46.

### Turkey




Number of respondents: 26.

Respondents could select up to three scenarios.
Source: Allianz Risk Barometer 2026.

## About Allianz Commercial

Allianz Commercial is the center of expertise and global line of Allianz Group for insuring mid-sized businesses, large enterprises and specialist risks. Among our customers are the world's largest consumer brands, financial institutions and industry players, the global aviation and shipping industry as well as family-owned and medium enterprises which are the backbone of the economy. We also cover unique risks such as offshore wind parks, infrastructure projects or film productions.

Powered by the employees, financial strength, and network of the world's #1 insurance brand, as ranked by Interbrand, we work together to help our customers prepare for what's ahead: They trust us to provide a wide range of traditional and alternative risk transfer solutions, outstanding risk consulting and multinational services as well as seamless claims handling.

The trade name Allianz Commercial brings together the large corporate insurance business of Allianz Global Corporate & Specialty (AGCS) and the commercial insurance business of national Allianz Property & Casualty entities serving mid-sized companies. We are present in over 200 countries and territories either through our own teams or the Allianz Group network and partners. In 2024, the integrated business of Allianz Commercial generated around €18 billion in gross premium globally.

## Further information and contacts

Please contact your regional Allianz Commercial contacts.

commercial.allianz.com

Email: az.commercial.communications@allianz.com

**Disclaimer & Copyright**

**Copyright © 2026 Allianz Commercial / Allianz Global Corporate & Specialty SE. All rights reserved.**

The material contained in this publication is designed to provide general information only. While every effort has been made to ensure that the information provided is accurate, this information is provided without any representation or warranty of any kind about its accuracy and neither Allianz Global Corporate & Specialty SE, nor any other company of Allianz Group can be held responsible for any errors or omissions.

All descriptions of insurance coverage are subject to the terms, conditions and exclusions contained in the individual policy. Any queries relating to insurance cover should be made with your local contact in underwriting and/or broker. Any references to third-party websites are provided solely as a convenience to you and not as an endorsement by Allianz of the content of such third-party websites. Neither Allianz Global Corporate & Specialty SE, nor any other company of Allianz Group is responsible for the content of such third-party websites and neither Allianz Global Corporate & Specialty SE, nor any other company of Allianz Group does make any representations regarding the content or accuracy of materials on such third-party websites.

Allianz Global Corporate & Specialty SE, Königinstraße 28, 80802 Munich, Germany.

Commercial Register: Munich, HRB 208312

February 2026