

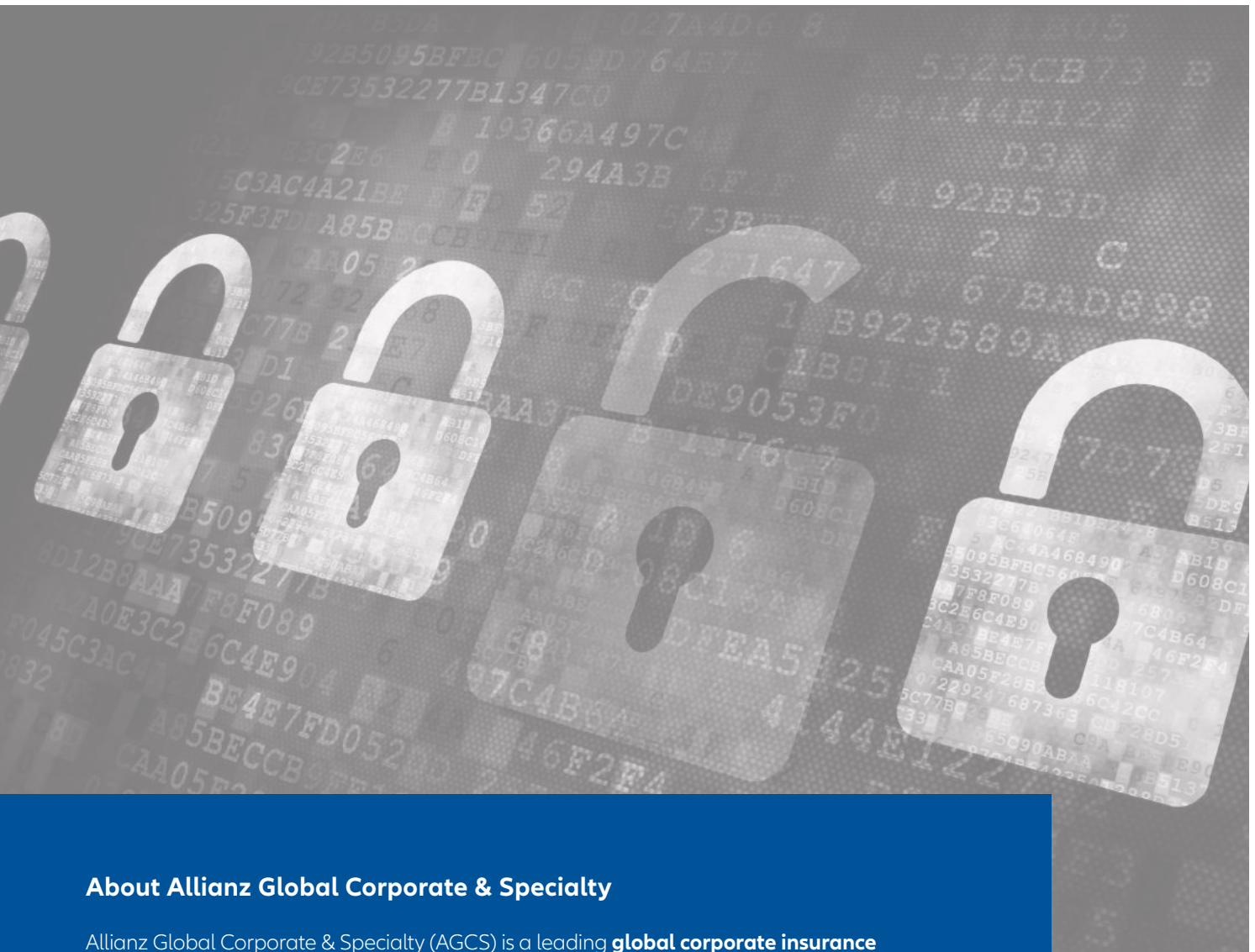


ALLIANZ RISK BAROMETER

IDENTIFYING THE MAJOR BUSINESS RISKS FOR 2020

The most important corporate perils for the next 12 months and beyond, based on the insight of more than 2,700 risk management experts from 102 countries and territories.





About Allianz Global Corporate & Specialty

Allianz Global Corporate & Specialty (AGCS) is a leading **global corporate insurance carrier** and a key business unit of Allianz Group. We provide **risk consultancy**, **Property-Casualty insurance solutions** and **alternative risk transfer** for a wide spectrum of commercial, corporate and specialty risks across 12 dedicated lines of business.

Our customers are as diverse as business can be, ranging from Fortune Global 500 companies to small businesses, and private individuals. Among them are not only the world's largest consumer brands, tech companies and the global aviation and shipping industry, but also wineries, satellite operators or Hollywood film productions. They all look to AGCS for smart answers to their largest and most complex risks in a dynamic, multinational business environment and trust us to deliver an outstanding **claims experience**.

Worldwide, AGCS operates with its own teams in **33 countries** and through the Allianz Group network and partners in over 200 countries and territories, employing over 4,400 people. As one of the largest Property-Casualty units of Allianz Group, we are backed by strong and stable **financial ratings**. In 2018, AGCS generated a total of €8.2 billion gross premium globally.

www.agcs.allianz.com/about-us/about-agcs.html

METHODOLOGY

The ninth **Allianz Risk Barometer** is the biggest yet, incorporating the views of a record 2,718 respondents from 102 countries and territories. The annual corporate risk survey was conducted among Allianz customers (global businesses), brokers and industry trade organizations. It also surveyed risk consultants, underwriters, senior managers and claims experts in the corporate insurance segment of both Allianz Global Corporate & Specialty (AGCS) and other Allianz entities.

Respondents were questioned during October and November 2019. The survey focused on large and small- to mid-sized enterprises. Respondents were asked to select the industry about which they were particularly knowledgeable and to name up to three risks they believed to be of the most importance.

Most answers were for large enterprises (>\$500mn annual revenue) [1,348 respondents 50%]. Mid-sized enterprises (\$250mn to \$500mn revenue) contributed 521 respondents (19%), while small enterprises (<\$250mn revenue) produced 849 respondents (31%). Risk experts from 22 industry sectors were featured.

Ranking changes in the Allianz Risk Barometer are determined by positions year-on-year not percentages.

All currencies US\$ unless stated.

[View the full regional, country and industry risk data](#)



2,718
respondents



102
countries



22
industry sectors

CONTENTS

03	Methodology
04	The Top 10 global business risks
06	Top business risks around the world
08	Executive summary
11	1. Cyber incidents
14	2. Business interruption
17	3. Changes in legislation and regulation
18	4-6 Business risk risers and fallers
19	Hot topic: 7 Climate change
22	8-10 Business risk risers and fallers
24	Contacts



2019: 37% (2)

Cyber incidents

(e.g. cyber crime, IT failure/outage, data breaches, fines and penalties)

[View the full Risk Barometer 2020 rankings here](#)



2019: 37% (1)

Business interruption

(incl. supply chain disruption)

KEY

▲ Risk higher than in 2019

▼ Risk lower than in 2019

■ No change from in 2019

(1) 2019 risk ranking

Source: Allianz Global Corporate & Specialty
 Figures represent the number of risks selected as a percentage of all survey response from 2,718 respondents.
 Figures don't add up to 100% as all respondents could select up to three risks per industry.

Ranking changes in the Allianz Risk Barometer are determined by positions year-on-year ahead of percentages.

1 Natural catastrophes ranks higher than market developments based on the actual number of responses



2019: 27% (4)

Changes in legislation and regulation

(e.g. trade wars and tariffs, economic sanctions, protectionism, Brexit, Euro-zone disintegration)

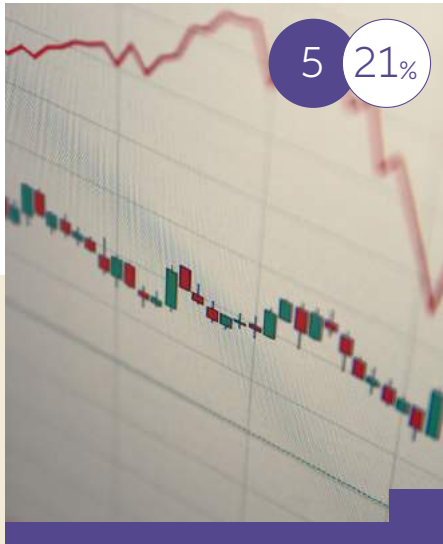


2019: 28% (3)

Natural catastrophes¹

(e.g. storm, flood, earthquake)

THE MOST IMPORTANT GLOBAL BUSINESS RISKS FOR 2020



2019: 23% (5)

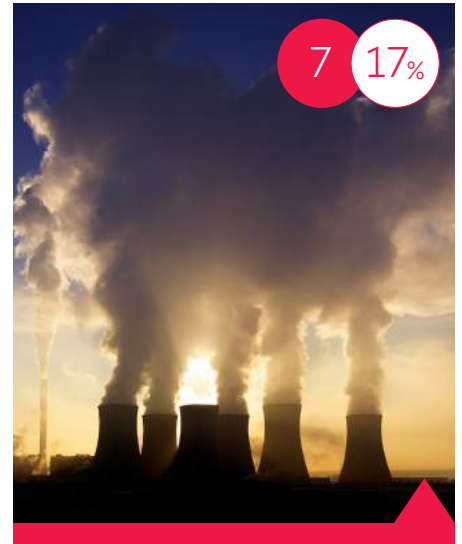
Market developments

(e.g. volatility, intensified competition/new entrants, M&A, market stagnation, market fluctuation)



2019: 19% (6)

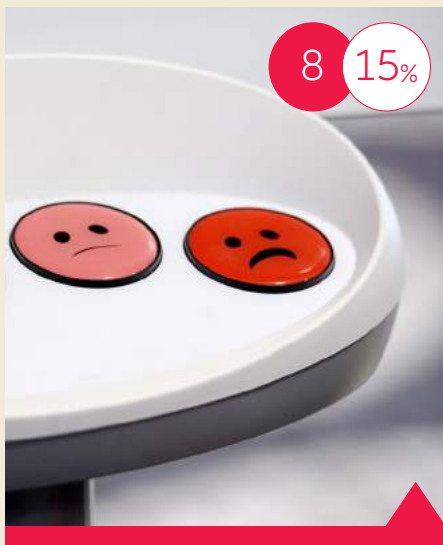
Fire, explosion



2019: 13% (8)

Climate change

/increasing volatility of weather



2019: 13% (9)

Loss of reputation or brand value



2019: 19% (7)

New technologies

(e.g. impact of Artificial Intelligence, autonomous vehicles, 3D printing, Internet of Things, nanotechnology, blockchain)



NEW

Macroeconomic developments

(e.g. monetary policies, austerity programs, commodity price increase, deflation, inflation)

ALLIANZ RISK BAROMETER 2020: TOP THREATS AROUND THE WORLD



Australia

- 1 **Changes in legislation/regulation** ■
- 2 **Cyber incidents** ▲
- 3 **Climate change** ▲

"The unprecedented number of major bushfires across multiple Australian states has dominated headlines. Fueled by rising temperatures and extreme dry weather attributed in part to climate change, these fires not only cause physical property damage, but also potential business interruption as the smoke causes hazardous air quality levels. With increased awareness, and first-hand experience of the negative impact, it is no surprise to see climate change in the top three Australian risks for the first time.

JAMES STACK, CEO AGCS AUSTRALIA

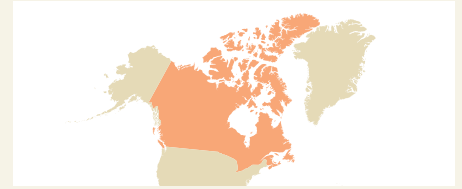


Brazil

- 1 **Business interruption** ▲
- 2 **Cyber incidents** ▼
- 3 **Fire, explosion** ▲

"The fact that business interruption has surpassed cyber incidents this year reflects how Brazilian companies still need to design contingency and recovery plans, as well as mitigate their risk exposures. Business Interruption claims can trigger several other claims, increasing losses exponentially"

GLAUCIA SMITHSON, CEO AGCS SOUTH AMERICA

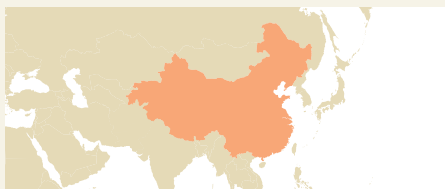


Canada

- 1 **Business interruption** ■
- 2 **Cyber incidents** ■
- 3 **Changes in legislation/regulation** ▲

"As expected, BI and cyber incidents continue to be major exposures for Canadian businesses. Changes in legislation and regulation has moved up significantly to 3rd, chosen as a top risk by almost a third of respondents. Trade wars, tariffs, economic sanctions and protectionism have companies concerned about the instability of future markets. We must ensure underwriters ask the right questions in order to understand today's risks and exposures and find solutions accordingly to help manage this uncertainty."

LINDA REGNER DYKEMAN, CHIEF AGENT, AGCS CANADA

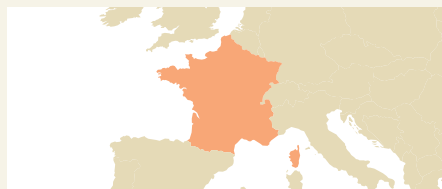


China

- 1 **Business interruption** ■
- 2 **Natural catastrophes** ■
- 3 **Cyber incidents** ▲

"With the country locked in a trade war with the US that does not look to be fully resolved any time soon, risk managers in China have chosen business interruption as their top risk, again, as the unpredictable nature of tariff announcements has made it difficult to plan accurately for the future. Also noteworthy is that cyber makes the top three risks for the first time, as businesses show a growing appreciation of the perils of non-traditional risks."

PATRICK ZENG, CEO AGCS HONG KONG AND GREATER CHINA



France

- 1 **Cyber incidents** ■
- 2 **Business interruption** ■
- 3 **Fire explosion** ■

"Cyber incidents, business interruption and fire/explosion remain the major concerns for companies in France. However, it's no surprise to see political risks/violence as a notable new entry in the top 10 risks as the 'yellow vests' movement and recent social strikes are affecting the French economy and businesses."

CORINNE CIPIERE, CEO AGCS FRANCE



Germany

- 1 **Business interruption** ■
- 2 **Cyber incidents** ■
- 3 **Changes in legislation/regulation** ■

"The reasons for business interruptions are becoming ever more diverse – fires, cyber incidents, but also political unrest in some countries. Above all, companies that rely heavily on suppliers – such as the German automotive industry – feel the impact of global connectedness and dependencies. That's why every business today not only needs to find answers to the question of how best to prevent business interruptions, but also how to best reduce their impact if they do happen."

HANS-JÖRG MAUTHE, CEO AGCS CENTRAL AND EASTERN EUROPE

[View all country, regional and industry risk data here](#)



 **Italy**

- 1 Business interruption ■
- 2 Cyber incidents ■
- 3 Loss of reputation or brand value ▲

"Loss of reputation or brand value has become a critical concern, entering the top three risks in Italy for the first time. However, business interruption and cyber incidents remain the major perils occupying the attention of Italian businesses."

NICOLA MANCINO, CEO AGCS ITALY

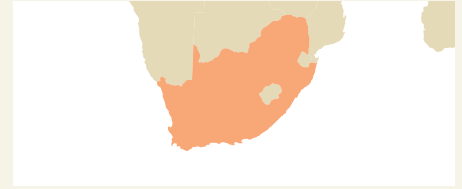



 **Singapore**

- 1 Business interruption ■
- 2 Cyber incidents ■
- 3 Changes in legislation/regulation ▲

"Changes in legislation and regulation cracks the top three business risks for Singaporean companies for the first time, reflecting the current unstable economic environment that businesses operate in as trade disputes such as the one between the US and China continue, as well as uncertainty over the eventual form of Brexit, dent confidence. Perennial leaders business interruption and cyber incidents continue to stress local risk managers, maintaining their positions as the number one and two top risks for businesses in Singapore following a year of major supply-chain disruptions and prominent data breach incidents."

MARK MITCHELL, CEO AGCS ASIA-PACIFIC

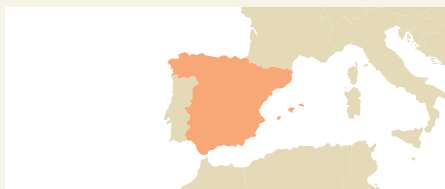


 **South Africa**

- 1 Cyber incidents ▲
- 2 Business interruption ▼
- 3 Changes in legislation/regulation ■

"Cyber incidents rises to the second top regional risk – and the top risk in South Africa – while companies are also more worried about changes in legislation and regulation, which remains at 3rd. The top risks in South Africa match the top three global risks, which shows African businesses have similar concerns as other companies around the world. Businesses across Africa are also increasingly concerned about business interruption as it has become the continent's top risk in 2020 from 5th in 2019. It also ranks in the top three risks in Tanzania (#1), Nigeria (#3), South Africa (#2) and Cameroon (#2)."

THUSANG MAHLANGU, CEO AGCS AFRICA

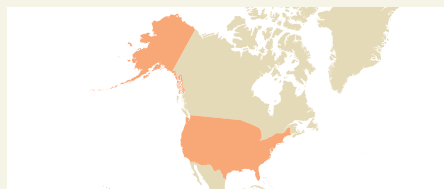


 **Spain**

- 1 Cyber incidents ▲
- 2 Business interruption ▼
- 3 Natural catastrophes ■

"The rise in the number of major cyber-attacks globally, as well as ransomware incidents that affected Spanish companies, has increased the awareness of cyber incidents which is now the top risk for the first time ever in Spain. In 2019, the country was affected by both extreme heat events and severe floods, causing increasing concerns for Spanish businesses, ensuring natural catastrophes remains in the top three risks."

JUAN MANUEL NEGRO, CEO AGCS SPAIN

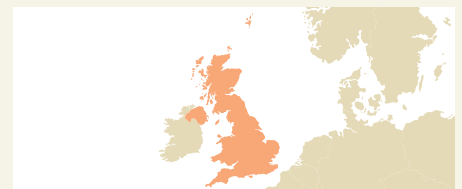


 **USA**

- 1 Cyber incidents ▲
- 2 Business interruption ▼
- 3 Natural catastrophes ■

"Cyber incidents has emerged as the top risk in the US and this is no surprise. Increasing connectivity and sophistication of attacks have been driving up the frequency and severity of incidents for some time. Given that most cyber-insurance is written in the US, this risk will continue to influence the direction of our industry and encourage close portfolio reviews of silent exposures."

BILL SCALDAFERRI, CEO AGCS NORTH AMERICA



 **UK**

- 1 Cyber incidents ■
- 2 Changes in legislation/regulation ▼
- 3 Business interruption ■

"Cyber incidents are on the rise and the survey results for the UK accurately reflect this as the top risk. While the uncertainty about changes in legislation such as Brexit continues, and is at the top of many board agendas, AGCS is continually looking at new and innovative ways to alleviate the many other business risks our insured partners are facing."

TRACEY HUNT, DEPUTY CEO, AGCS UK

EXECUTIVE SUMMARY



The 10 top concerns of risk management experts

Cyber incidents ranks as the top peril for companies globally in the **Allianz Risk Barometer** for the first time after receiving 39% of responses from more than 2,700 risk management experts in over 100 countries and territories – the largest number of respondents ever. Seven years ago cyber risk ranked only 15th with just 6% of responses. Awareness of the cyber threat has grown rapidly in recent years, driven by companies' increasing reliance on their data and IT systems and a number of high-profile incidents.

Businesses face a growing number of cyber challenges including larger and more expensive data breaches, an increase in ransomware and business email compromise (spoofing) incidents, as well as the prospect of litigation after an event. Political differences between nation states being played out in cyber space brings added risk complexity, while even a successful merger or acquisition (M&A) can result in systems problems. [▶ Page 11](#)

Data breaches are the main cause of cyber incidents, according to **Allianz Risk Barometer** respondents. And as companies collect and use ever greater volumes of personal data, breaches are becoming larger and costlier. Dealing with a mega breach (involving more than one million records) now costs \$42mn on average¹ – up 8% year-on-year. Breaches in excess of 50 million records cost \$388mn on average – up 11%. Data protection and privacy regulation, and subsequent penalties, are widening in scope and geographical reach – in the UK two £100mn (\$130mn) fines were issued by the regulator in July 2019 alone. The General Data Protection Regulation (GDPR) which came into force in Europe in 2018 will likely bring a further wave of fines in 2020. Over 200,000 cases were reported in the first nine months of its implementation.

Meanwhile, litigation is also starting to impact costs and a number of large breaches have triggered class actions by consumers or investors. In July 2019, Equifax reached a \$700mn settlement for a mega breach in 2017.

Ransomware incidents are becoming more damaging, increasingly targeting large companies with sophisticated attacks and hefty extortion demands. Five years ago, a typical demand would have been in the tens of thousands of dollars. Now it can be in the millions. Industrial and manufacturing firms are increasingly targeted but losses tend to be highest for law firms, consultants and architects, for which IT systems and data are their life blood. Spoofing attacks are also increasing in frequency. Such incidents, which involve social engineering and phishing emails to dupe companies' employees into revealing login credentials or to make fraudulent transactions, have resulted in worldwide losses of \$26bn since 2016 according to the FBI. [▶ Page 12](#)

Cyber exposures are also emerging as a hot M&A topic in the wake of a number of large data breaches. A 2018 breach experienced by the Marriott hotel chain was traced to an intrusion in 2014 at Starwood, a hotel group it acquired in 2016. Even the best protected companies will be exposed if they acquire a company with existing vulnerabilities and the acquiring firm could be liable for any incidents pre-dating the merger. Considering potential cyber vulnerabilities and exposures needs to become a higher priority for businesses conducting M&A. [▶ Page 13](#)

The involvement of nation states in cyber-attacks also poses a growing risk for companies, which can be targeted for intellectual property or by groups intent on causing disruption or physical damage. Tensions in the Middle East have seen

¹ IBM Security, Ponemon, Cost Of A Data Breach Report 2019



international shipping hit by attacks in the Persian Gulf. Oil and gas installations have also been affected.

Preparation and training are the most effective forms of cyber risk mitigation and can significantly reduce the consequences of an event. Many incidents are the result of human error, which can be mitigated by training, especially in areas like phishing and spoofing, which are among the most common forms of attack. Training can also help mitigate ransomware attacks, although maintaining secure backups can limit damage. Business resilience and business continuity planning are also crucial although response plans need to be tested and regularly reviewed.

After seven years at the top, **business interruption (BI)** drops to second position in the **Allianz Risk Barometer** (37% of responses). However, the trend for larger more complex BI losses – from both traditional causes, such as fires – the average insured BI loss from a fire is €5.8mn (\$6.7mn), 45% higher than the corresponding property damage² – and natural catastrophes, as well as newer causes, such as technical issues with digital supply chains and platforms or even civil unrest, continues unabated. [▼ Page 14](#)

Contingent business interruption (CBI) events (whereby a company suffers a loss due to an event at a customer or supplier) are now far larger and more widespread than 10 or even five years ago and can impact multiple companies and countries. Industries such as automotive manufacturing and pharmaceuticals may have developed highly efficient global supply chains, but this also makes them vulnerable to large BI and CBI events. Furthermore, other industries are now emulating such supply chains.

Businesses are increasingly exposed to the direct and indirect impact of political risk exposures such as riots and civil unrest and terrorism attacks, which can result in huge disruption. The past year has seen civil unrest escalate in Hong Kong, Chile, France, Bolivia and Colombia resulting in property damage, BI and a general loss of income for many companies. In Chile protests which began in October 2019 resulted in hundreds of supermarkets being looted or set on fire. The damage bill is currently in the region of \$3bn with many businesses unable to reopen for months. In Hong Kong the ongoing social unrest has resulted in a 40% year-on-year drop in tourists. Another consequence of such events is that employees might not be able to access their workplace which can bring production to a standstill in many industries. Insurers are seeing an uptake in specialist political violence or riot insurance which can mitigate the consequences of such disruptions. [▼ Page 15](#)

In future, businesses are also likely to face an increased risk of disruption from extreme weather activity which can affect the availability of resources, such as water or power. In 2018, low water levels on the Rhine made parts of the river unnavigable, causing a number of manufacturers to cease production. Even mitigation measures can also cause BI – drought conditions in 2019 led utility suppliers in California to carry out planned power outages to reduce the risk of wildfires. Certain industries are also becoming more concerned about continuity of supply of key ingredients in modern food supply chains. In 2018, a shortage of carbon dioxide created disruption in the food and beverage sector at a time of peak summer demand. Droughts, heatwaves and floods have affected yields of vegetables, wheat and milk in recent years, affecting supplies for food manufacturers and retailers. Large companies are increasingly

² Allianz Global Corporate & Specialty, Based on the analysis of 1,175 corporate insurance claims between July 2013 and July 2018 that have both a property damage and business interruption component

looking to protect their balance sheets from the growing number of BI scenarios with more tailored insurance solutions. [↘ Page 16](#)

Businesses are more concerned about **changes in legislation and regulation** (3rd, 27%) than a year ago with this risk appearing in the top three for the first time. Tariffs, sanctions, Brexit and protectionism – around 1,300 new trade barriers were implemented in 2019 alone – were cited as key concerns by respondents. Companies face other major challenges in 2020 such as “game-changing” sustainability regulation in Europe. Increasingly, companies and investors are considering sustainability credentials when it comes to choosing business partners. [↘ Page 17](#)

Devastating typhoons in Asia and record-breaking wildfires in Australia were among the disasters which made headlines in 2019. However, economic losses from **natural catastrophes** actually declined 20% year-on-year to around \$130bn, meaning this peril drops out of the top three global risks for the first time (4th, 21%). However, **climate change** (7th 17%) rises to its highest-ever position in the **Allianz Risk Barometer**. Global warming fuels extreme calamities worldwide and threatens populations and business. Rising seas, drier droughts, fiercer storms and massive flooding pose physical threats to firms because they imperil factories and other assets, as well as transport and energy links which tie supply chains together. An increase in physical losses is the exposure businesses fear most, according to respondents, and the growing cost is already noticeable. The number of weather-related/flood loss events has increased by a factor of three to four since 1980. There are 16,000 fatalities in G20 economies alone due to extreme weather events every year with the economic impact estimated to be \$142bn, according to Climate Transparency³. [↘ Page 18](#)

Companies are realizing they may face criticism, reputational damage and increasing regulatory and legal action if they don't adequately address climate change in their operations. It is estimated that around 1,500 new laws are being introduced around the world every year in response to climate change but it is not just governments and regulators who are applying pressure. Climate-linked activism against corporates is on the rise – particularly in Europe – and boards are increasingly challenged by investors and other stakeholders.

Failure to disclose climate change risk will drive more litigation in future. Climate change cases have already been brought in over 30 countries around the world to date with three-quarters of

cases filed in the US. Many lawsuits target the “carbon majors” – active fossil fuel producers. However, this will likely expand to other carbon-heavy industries, such as agri-business, manufacturing and transport. Combatting climate change requires corrective action and investment, but it also brings opportunities for new business models and markets, such as renewable energy, rare earth mining and battery production, for example. [↘ Page 19](#)

Market developments (5th 21%) and **fire, explosion** (6th 20%) occupy the same positions as in 2019. [↘ Page 18](#)

However, **loss of reputation or brand value** is another peril to rise up the **Allianz Risk Barometer** year-on-year (8th, 15%). Corporate scandals involving reputation can originate from a growing number of scenarios. The impact of reputation events on stock prices is believed to have doubled since the introduction of social media. Many companies are still inadequately protected against the consequences of a reputational crisis. Effective planning has become essential and a professional response can make a difference. Insurance can also provide tangible assistance to an intangible risk, providing solutions such as protection against reduced net operating profit, rectification advice costs and a 24/7 reputational crisis response. [↘ Page 22](#)

New technologies (9th, 13%) such as Artificial Intelligence (AI) present considerable opportunities for businesses. In the insurance industry, AI applications will improve the transaction process, with many benefits already apparent. Customer needs can be better identified. Policies can be issued, and claims processed more quickly and cheaply. Large corporate risks, such as BI, cyber security threats or macroeconomic crises, can be better predicted. However, new technologies also bring risks. According to **Allianz Risk Barometer** respondents, the increasing utilization of AI and digital platforms are the innovations that also come with the greatest future risk potential. With AI, lack of transparency or human oversight may result in unpredictable outcomes creating complex liability issues. If a digital platform is unavailable due to a technical glitch or cyber event, the losses for multiple companies reliant on it could be in the hundreds of millions of dollars or higher if they cannot provide services or products. [↘ Page 22](#)

Macroeconomic developments is a new entry in the top 10 risks for 2020 (10 11%), driven by corporate fears over a global recession and debt accumulation, particularly in the US and China, notably with regards to the private sector. [↘ Page 23](#)

³ Climate Transparency, Brown To Green, The G20 Transition Towards A Net-Zero Emissions Economy 2019



39% ▲ 2019: 2 (37%)

1 CYBER INCIDENTS

(e.g. cyber crime, IT failure/outage, data breaches, fines and penalties)

Cyber risk tops the Allianz Risk Barometer for the first time with businesses facing a number of challenges such as larger and costlier data breaches, more ransomware incidents and the increasing prospect of litigation after an event. The playing out of political differences in cyber space also ups the ante while even a successful M&A can result in unexpected problems.

Ranking history (% of responses and position):

2018 2 (40%)
2017 3 (30%)
2016 3 (28%)
2015 5 (17%)

Top risk in:

- 🇦🇹 Austria
- 🇧🇪 Belgium
- 🇫🇷 France
- 🇮🇳 India
- 🇲🇾 Malaysia
- 🇿🇦 South Africa
- 🇰🇷 South Korea
- 🇪🇸 Spain
- 🇸🇪 Sweden
- 🇨🇭 Switzerland
- 🇬🇧 UK
- 🇺🇸 USA

Top risk in the following sectors:

- ✈️ Aviation
- 🏦 Financial Services
- 🏛️ Government & Public Services
- 👨‍💻 Professional Services
- 🖥️ Technology
- 📞 Telecommunications

In 2020, **cyber incidents (39% of responses)** ranks as the most important business risk in the **Allianz Risk Barometer**. Compare this with 2013, when it finished 15th with just 6% of responses and it is clear how quickly awareness of the cyber threat has grown, driven by companies' increasing reliance on their data and IT systems.

Cyber risks continue to evolve. A significant increase in the number of ransomware incidents is helping to drive up the frequency of losses for companies. Overall, cyber-attacks are becoming more sophisticated and targeted as criminals seek higher rewards with multimillion dollar extortion demands.

"The costs of a cyber incident are rising across the board, a product of growing complexity, more stringent regulation and the damaging consequences to a business from a loss of data or critical systems," says **Marek Stanislawski, Deputy Global Head of Cyber at AGCS**. "In particular, the cost of large data breaches continues to increase, as data protection and privacy regulation widen in scope and geographical reach and class action litigation also starts to impact the cost of dealing with a

breach. Meanwhile, when an incident leads to significant business interruption (see page 14), losses are typically high."

TREND

DATA BREACHES LARGER AND MORE EXPENSIVE

As companies collect and use ever greater volumes of personal data, data breaches are becoming larger and costlier. In particular, so-called mega data breaches (involving more than one million records) are more frequent and expensive. In July 2019, Capital One revealed it had been hit by one of the largest ever breaches in the banking sector with approximately 100 million customers impacted. Yet this breach is by no means the largest in recent years.

Data breaches at hotel group Marriott in 2018 and credit score agency Equifax in 2017 were reported to have involved the personal data of over 300 million and 140 million customers respectively. Both companies faced numerous law suits and regulatory actions in multiple jurisdictions – the UK's data protection regulator intends to fine Marriott £100mn

WHAT ARE THE MAIN CAUSES OF CYBER INCIDENTS?



1. Data or security breach
(e.g. access to/deletion of personal/confidential information)



2. Espionage, hacker attack, ransomware, denial of service



3. Errors or mistakes by employees

“More and more events – from leaving a laptop with confidential data on a train to losing a customer list – can constitute a data breach,” says Marek Stanislawski, Deputy Global Head of Cyber at AGCS. **“It is estimated that anywhere between 50% and 90% of breaches are caused or abetted by employees, be it by simple error or by falling victim of phishing or social engineering. Well-trained and vigilant employees can become an extension of a company’s cyber security team and help form a much firmer perimeter around the company’s assets.”**

Source: Allianz Global Corporate & Specialty

Figures represent the percentage of answers of all participants who responded (1,071). Figures don't add up to 100% as up to three risks could be selected

(\$130mn) for the breach, among the earliest and largest fines under the EU's new privacy laws to date.

In the same month – July 2019 – British Airways was provisionally fined £183mn (\$240mn) for a data breach impacting 500,000 customers in 2018.

The General Data Protection Regulation (GDPR) rules that came into force across Europe in 2018 will likely bring further fines in 2020. The European Data Protection Board (EDPB) released a preliminary report¹ stating that of the 206,326 cases reported under the GDPR across 31 countries in the first nine months of its implementation, the national data protection agencies had only resolved around 50% of them. As shown above, as regulators have worked through this backlog, more fines of greater amounts have been recorded.

A mega breach now costs an average of \$42mn², according to the Ponemon Institute, an increase of nearly 8% over 2018. For breaches in excess of 50 million records, the cost is estimated to be \$388mn (11% higher than in 2018).

TREND RANSOMWARE BRINGS INCREASING LOSSES

According to the EU's law enforcement agency, Europol, ransomware is the most prominent cyber crime threat.

Already high in frequency, incidents are becoming more damaging, increasingly targeting large companies with sophisticated attacks and hefty extortion demands. “Five years ago, a typical ransomware demand would have been in the tens of thousands of dollars. Now they can be in the millions,” says Stanislawski.

The consequences of an attack can be crippling, especially for organizations that rely on data to provide products and services. Extortion demands are just one part of the picture. Business interruption brings the most severe losses from ransomware attacks and in some cases ransomware is a smoke screen for the real target, such as the theft of personal data. Industrial and manufacturing firms are increasingly targeted but losses tend to be highest for law firms, consultants and architects, for which IT systems and data are their life blood.

Incidents such as those featuring the **Ryuk malware** have emerged as a key driver for cyber insurance claims in recent years. Named after a fictional manga character, it was first reported in August 2018 and has been responsible for multiple attacks against large companies, hospitals and local governments globally.

TREND BEC ATTACKS RESULT IN BILLION DOLLAR FRAUD

Business email compromise (BEC) – or spoofing – attacks are increasing in frequency. BEC incidents have resulted in worldwide losses of at least \$26bn since 2016 according to the FBI in the US.

Such attacks typically involve social engineering and phishing emails to dupe employees or senior management into revealing login credentials or to make fraudulent transactions.

TREND LITIGATION PROSPECTS RISING

Many large data breaches today spark regulatory actions, but they can also trigger litigation from affected consumers, business partners and investors. When they do, legal expenses can add substantially to the cost.

Data breach litigation in the US is a developing situation. A number of large breaches have triggered class actions by consumers or investors – in July 2019, Equifax reached a \$700mn settlement for its 2017 mega breach. US courts have been battling the questions of “legal standing” – whether claimants have the right to

¹ European Data Protection Board, First Overview On The Implementation Of The GDPR And The Roles And Means Of The National Supervisory Authorities

² IBM Security, Ponemon, Cost Of A Data Breach Report, 2019

sue – but the trend appears to be favoring plaintiffs. Statutory and regulatory changes could also facilitate compensation for data breaches. The California Consumer Privacy Act, for example, provides a mechanism for consumers to sue businesses and – in a first for the US – sets statutory damages for data breaches.

Outside the US, a number of countries have expanded group action litigation rights. For example, in Europe, the GDPR makes it easier for victims of a data or privacy breach to seek legal redress.

In addition, claimant law firms and litigation funders are actively looking to bring class actions for data breaches in Europe and elsewhere – a class action against British Airways following its 2018 data breach was recently given the go-ahead in the UK courts. Consumer groups are also looking to test the GDPR and challenge some organizations' interpretation of the new law.

TREND **M&A CAN BRING CYBER ISSUES**

Cyber exposures have emerged as a hot topic in mergers and acquisitions (M&A) following some large data breaches. For example, the 2018 Marriott breach was traced to an intrusion in 2014 at Starwood, a hotel group it acquired in 2016.

Even the best protected companies will be exposed if they acquire a company with weak cyber security or existing vulnerabilities. The acquiring firm could be liable for any damage from incidents which pre-date the merger.

Ultimately, considering potential cyber vulnerabilities and exposures needs to become a higher priority for businesses during M&A, as many companies are not doing enough due diligence in this area. At the same time, once a deal has been completed many companies do not address any weaknesses in acquired systems quickly enough.

TREND **POLITICAL FACTORS PLAY OUT IN CYBER SPACE**

The involvement of nation states in cyber-attacks is increasing risk for companies, which are being targeted for intellectual property or by groups intent on causing disruption or physical damage. For example, growing tensions in the Middle East have seen international shipping targeted by spoofing attacks in the Persian Gulf while oil and gas installations have been hit by cyber-attacks and ransomware campaigns.

WHAT IS THE BEST APPROACH TO MANAGING CYBER RISK AND IMPROVING CYBER RESILIENCE?



“Purchasing cyber insurance should be one of the final points in a company’s plan to enhance its cyber resilience,” says Marek Stanislawski, Deputy Global Head of Cyber at AGCS. “Insurance has a vital role to play in helping companies recover if all other measures are insufficient but it should not replace strategic risk management. Investing in employee awareness, together with updating and continuous monitoring of systems should definitely be at the top of any company’s cyber to-do list.”

Source: Allianz Global Corporate & Specialty
Figures represent the percentage of answers of all participants who responded (1,071). Figures don't add up to 100% as up to three risks could be selected

Sophisticated attack techniques and malware may also be filtering down to cyber criminals while nation state involvement is providing increased funding to hackers. Even where companies are not directly targeted, state-backed cyber-attacks can cause collateral damage. In 2017 the **NotPetya malware** attack primarily targeted the Ukraine but quickly spread around the world.

RISK MITIGATION

Preparation and training are the most effective forms of mitigation and can significantly reduce the likelihood or consequences of a cyber event. Many incidents are the result of human error, which can be mitigated by training, especially in areas like phishing and business email compromise, which are among the most common forms of cyber-attack.

Training could also help mitigate ransomware attacks, although maintaining secure backups can also limit the damage from such incidents. Business resilience and business continuity planning are also key to reducing the impact of a cyber incident, although response plans need to be tested, practiced and regularly reviewed.

➤ For more information on cyber risk and insurance



37% ▼ 2019: 1 (37%)

2 BUSINESS INTERRUPTION

(incl. supply chain disruption)

Fires and natural catastrophes are the major causes of business interruption losses – which can cost as much as 45% more than the corresponding property damage from such incidents. However, more exotic triggers like digital platforms and supply chains, political risks and environmental factors are also becoming more relevant for businesses.

Ranking history (% of responses and position):

2018 1 (42%)
2017 1 (37%)
2016 1 (38%)
2015 1 (46%)

Top risk in:

- 🇦🇹 Austria
- 🇧🇷 Brazil
- 🇨🇦 Canada
- 🇨🇳 China
- 🇨🇴 Colombia
- 🇩🇪 Germany
- 🇮🇩 Indonesia
- 🇮🇹 Italy
- 🇲🇾 Malaysia
- 🇳🇱 Netherlands
- 🇵🇭 Philippines
- 🇵🇱 Poland
- 🇸🇬 Singapore
- 🇹🇿 Tanzania

Top risk in the following sectors:

- 🏭 Chemicals, Pharmaceuticals, Biopharma
- 🍷 Food & Beverages
- 🏭 Heavy Industry
- 🏭 Manufacturing (incl. Automotive)
- 🛢️ Oil & Gas
- ⚡ Power & Utilities
- ☀️ Renewable Energy
- 🛒 Retailing, Wholesale
- 🚚 Transportation

For seven years in a row the impact of **business interruption (incl. supply chain disruption)** has ranked as the most important risk for companies in the **Allianz Risk Barometer**. In 2020 it is finally replaced in top position by cyber incidents, a peril with which it is closely interlinked.

It may no longer be the standalone number one peril in the eyes of risk management experts but the business interruption (BI) threat is undiminished. The trend for larger more complex BI losses – from both traditional causes, such as fires and natural catastrophes, and newer ones, such as digital supply chains or civil unrest – continues unabated.

Contingent business interruption (CBI) events (whereby a company suffers a loss due to an event at a customer or supplier) are now far larger and more widespread than 10 or even five years ago. In recent years, natural catastrophes, fires and cyber-attacks have all caused large CBI loss events that have impacted multiple companies in multiple countries. Industries such as automotive manufacturing and pharmaceuticals may have developed highly efficient global supply chains, but this also makes them vulnerable to very large BI and CBI events. For example, a fire at an auto-parts manufacturing plant in the US in 2018 caused supply shortages for a number of car manufacturers and was the catalyst for hundreds

of millions of losses throughout the industry. A year earlier, another fire at an auto-part manufacturer in the Czech Republic had a similar impact. Furthermore, a growing number of other industries are now emulating such supply chains.

TREND

DATA VULNERABILITIES AND DIGITAL SUPPLY CHAIN REACTIONS

The growing reliance on technology and data from business is beginning to manifest in BI and CBI claims. Companies can suffer major BI losses due to the unavailability of critical data or technology, either through a technical glitch, cyber-attack or a physical event, such as fire or flood.

Loss of data, or “business intelligence”, is emerging as a significant cause of loss. The inability to access data for an extended period of time can have a significant impact on revenues – for example, if a company is unable to take orders. One notable large BI claim in 2019 involved a fire at a European media company. A significant proportion of the claim was related to the unavailability of data and the cost of restoration.

Dependency on digital supply chains – both for the delivery of services and the supply of goods – brings numerous benefits. Shared technology-based platforms enables data to be exchanged

between parties, automates administrative tasks and orders and transports products on demand. Digital supply chains are more transparent and goods can be tracked back to their source. For example, the food and pharmaceutical industries are just two sectors that are already using blockchain solutions to trace ingredients and products as they move through the supply chain.

However, such platforms can potentially create a chain reaction ensuring a BI cascades through a whole sector. If a platform is unavailable due to a technical glitch or cyber event, it could bring large BI losses for multiple companies that all rely and share the same system. In June 2019, an outage caused a catastrophic failure at some Google cloud services, causing several hours of disruption to a number of large online service providers, including YouTube, Uber and Snapchat. In 2017, a four-hour outage at Amazon Web Services in North America was estimated to have cost S&P 500 companies \$150mn.

“Digital supply chains can be more efficient and traceable, but a fire at a data center or a hack could cause a significant BI and it may no longer be possible to switch back to manual processes if the system is down,” says **Raymond Hogendoorn, Global Head of Property and Engineering Claims at AGCS**. “By making supply chains digital, organizations also make themselves more vulnerable to BI.”

TREND POLITICAL VIOLENCE BI IS UNDERESTIMATED

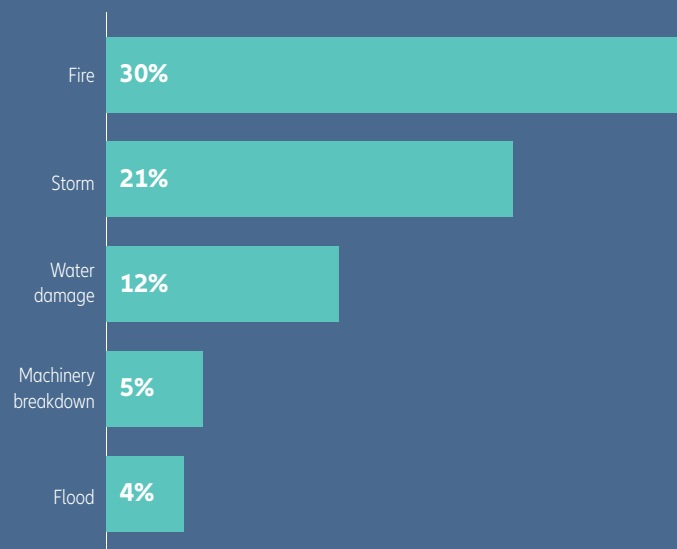
In today’s volatile world, businesses are increasingly exposed to political risk exposures in their many guises – riots and civil unrest, strikes and, of course, terrorism attacks, can cause huge disruption to companies.

The past year alone has seen civil unrest in Hong Kong, Chile, France, Bolivia and Colombia to name just a few examples, resulting in property damage, BI and a general loss of income for many businesses.

“Political BI risk is often underestimated,” says Hogendoorn. “Ten years ago, protests in somewhere like Chile may have gone largely unnoticed by global businesses, but today the impact of such events is all too apparent.”

The protests against the Chilean government began in October 2019 and have resulted in a number of deaths, thousands of injuries and significant damage to property. Hundreds of supermarkets have been looted or set on fire with

WHAT ARE THE MOST FREQUENT CAUSES OF BUSINESS INTERRUPTION INSURANCE CLAIMS?



According to AGCS, fire and explosion incidents are the most frequent cause of business interruption loss, accounting for almost a third (30%) of claims by number. BI costs following a fire can significantly add to the final loss total. For example, the average BI loss from a fire or explosion incident is €5.8mn (\$6.7mn) compared to €4mn (\$4.5mn) for the average direct property loss¹ or 45% higher.

Source: Allianz Global Corporate & Specialty. Based on the analysis of 1,175 corporate insurance claims between July 2013 and July 2018 with a total value of €6.3bn (\$7.1bn) that have both a property damage (€2.6bn) and business interruption (€3.7bn) component.

the property and transport damage bill currently estimated to be in the region of \$3bn. Retail giant Walmart is among those who have suffered significant losses.

“Even if it was ‘just’ looting it will still take several months until the supermarkets can open again, so there are enormous BI losses,” says **Bjoern Reusswig, Head of Global Political Violence and Hostile Environmental Solutions at AGCS**. “This event is predicted to be one of the biggest losses in the history of political violence insurance.”

Political risks can also result in BI losses even if there is no physical damage. In Hong Kong, the ongoing social unrest has resulted in a 40% year-on-year drop in tourism with serious ramifications for the industry.

“It’s not only that customers or hotel guests stay away,” says Reusswig. “Another consequence of these types of events is that employees might not be able to access their workplace because of security reasons. This can reduce productivity or bring production to a standstill in other industries.”

¹ Based on the analysis of 354 fire claims between July 2013 and July 2018 with a total value of €3.5bn (\$4bn) that have both a property damage (€1.4bn) and business interruption (€2.1bn) component.

In Hong Kong, purchasing of political violence or riot insurance is relatively uncommon so many companies will be left to foot any damage or disruption bill themselves. However, globally, insurers are seeing an increase in BI losses from political risks, in part because customers are buying more insurance – particularly so-called denial of access and loss of attraction coverage – but also because companies and supply chains are increasingly international.

TREND
ENVIRONMENTAL DRIVERS ON THE HORIZON

Businesses are likely to face an increased risk of disruption from extreme weather activity and environmental factors in future. Globalization and supply chain dependencies have helped make BI a much larger proportion of natural catastrophe losses today than was the case even 10 or 20 years ago. A storm in Japan or an earthquake in Chile can affect production at a manufacturing plant in Europe.

Extreme weather can also affect the availability of resources, such as water or power – with unexpected consequences. In 2018, low water

levels on the Rhine made parts of the river unnavigable, causing a number of manufacturers to cease production. Even measures to mitigate weather events and climate change can also cause BI – drought conditions in 2019 led utility suppliers in California to carry out planned power outages to reduce the risk of wildfires.

Businesses may even need to relocate or find alternative suppliers, for example, if a manufacturing or industrial facility is no longer accepted in a residential area or due to an increased risk of flooding. Certain industries are also becoming more concerned about continuity of supply of key ingredients, in particular in the context of modern food supply chains. In 2018, a shortage of carbon dioxide created disruption in the food and beverage sector at a time of peak summer demand. Extreme weather can lead to volatility in the supply of certain foods. Droughts, heatwaves and floods in recent years have affected yields, including vegetables, wheat and milk, affecting supplies for food manufacturers and retailers.

“Companies are increasingly thinking about how extreme weather events affect supply chain risk and how this can be managed,” says **Georgi Pachov, Global Property Practice Leader, Cyber at AGCS**. “There are companies in the food and beverage industry enquiring about BI linked to key ingredients in their products and how this might be captured in insurance. The challenge for the insurance industry is to ensure the BI solutions of the future are fit for purpose.”

MITIGATION
A SHIFT TO BESPOKE BI COVERAGE

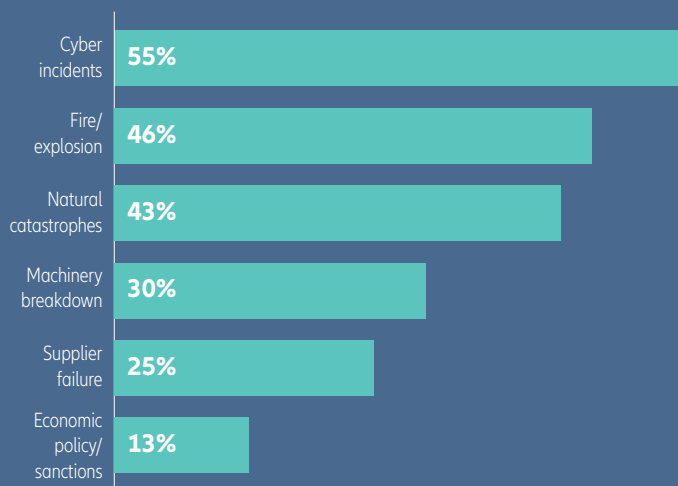
At a time when many industries and supply chains are becoming more sensitive to BI, shareholders and customers are also becoming more risk averse and less forgiving of nasty surprises. As a result, large companies are increasingly looking to protect their balance sheets with more tailored BI solutions.

“We see a growing demand for BI solutions that protect a company’s balance sheet,” says Pachov. “These may not be traditional BI triggers, such as fire and nat cats, but protection against risks which complement the business model and strategy for two, three or four years ahead.

“The BI insurance solution of five years’ time will be much more bespoke than it is currently, incorporating data-driven insights into the solution development and placement. We are increasingly entering into partnerships with clients to protect the balance sheet from a wider range of BI risk.”

➤ [For more information on business interruption insurance solutions](#)

WHAT CAUSES OF BUSINESS INTERRUPTION DO YOU FEAR THE MOST?



“Today, many companies’ supply chains are much more integrated, so the financial impact of a BI is becoming larger and larger,” explains **Raymond Hogendoorn, Global Head of Property and Engineering Claims at AGCS**. **“An incident like a fire or a cyber- attack at one company can affect the entire supply chain impacting multiple manufacturers.”**

Source: Allianz Global Corporate & Specialty. Figures represent the percentage of answers of all participants who responded (1,018). Figures don’t add up to 100% as up to three risks could be selected.

Brexit is still a major concern for businesses

3. Changes in legislation and regulation



27% ▲ 2019: 4 (27%)

3

CHANGES IN LEGISLATION AND REGULATION

(e.g. trade wars and tariffs, economic sanctions, protectionism, Brexit, Euro-zone disintegration)

Hopes that the US-China trade dispute would ease did not materialize in 2019. Protectionism became the new normal with around 1,300 new trade barriers implemented. Meanwhile, companies will face major challenges in 2020, such as game-changing EU sustainability regulation.

Top risk in:

- Australia
- Bulgaria
- Colombia
- Croatia
- Hungary
- Russia

The world's two largest economies have been locked in a bitter trade battle for over 18 months now with the US and China imposing tariffs on hundreds of billions of dollars' worth of one another's goods. The US-China trade dispute has brought the US average tariff to 8% – close to levels last seen in the 1970s – from 3.5% at the end of 2017. At the same time, a higher share of global trade is also now being tariffed.

Partly in reaction to this trend, the European Union (EU) has taken the opposite stance, aggressively promoting its trade model – freer and greener – as evidenced by the implementation of the EU-Japan Free Trade Agreement and the EU-Singapore Free Trade Agreement, as well as the finalization of negotiations of the EU-Vietnam or the EU-Mercosur states (Argentina, Brazil, Paraguay and Uruguay) agreements a few months before the end of the European Commission's mandate. "Trade policy is becoming just another political tool for many different policy ends, such as economic diplomacy, geopolitical influence or environmental policy," explains **Ludovic Subran, Chief Economist of Allianz**. "This activism is not restricted to the US: it has spread to Japan and South Korea, India and the EU."

Meanwhile, companies will face major regulatory challenges in 2020. "The EU Sustainability Regulation is nothing less than a game changer,"

says Subran. "The impact on corporates will be as wide-ranging as new rules on accounting and data protection were in the past."

Mainstreaming sustainability into risk management basically means that all businesses have to develop a clear Environmental, Social and Governance (ESG)-profile by disclosing their ESG-risks as well as opportunities, using state-of-the-art methodologies and techniques. At the heart of the process is the de-carbonization drive, i.e. defining a clear path to carbon-neutrality by 2050. Many countries have already enshrined this goal by law and many more will follow in the coming years, including – very likely – the EU. For many corporates, the process of data gathering, target-setting and measurement implementation will be a cumbersome one – but one which also provides huge opportunities. "Increasingly, companies and investors alike – not least driven by their own regulatory constraints – will choose their business partners by their sustainability credentials," says Subran. "Corporates that anticipate the coming sustainability regulation will be ahead of the curve in competition."

"Sustainability is the name of the game for staying in business and prospering. And not only in Europe. The EU might be spearheading regulation in this field, but, as with other EU initiatives, Europe's sustainability regulation is set to become a global standard rather quickly."

4

NATURAL CATASTROPHES

(e.g. storm, flood, earthquake)

21% ▼ 2019: 3 (28%)

Devastating typhoons in Asia and record-breaking wildfires in Australia were among the disasters which dominated global headlines in 2019. However, economic losses from natural catastrophe events actually declined 20% year-on-year to around \$133bn, according to reinsurer Swiss Re¹. Insured losses also fell to \$50bn from \$84bn, driven by Hurricane Dorian in North America (\$4.5bn) and typhoons Faxai (\$7bn) and Hagibis (\$8bn) in Japan.

"2019 was another year without a single major nat cat event comparable in economic loss size with those of the 2017 Atlantic hurricane season (the costliest on record)," says **Carina Pfeuffer, Cat Risk Analyst, AGCS**. "Rather, aggregated

losses from multiple small- to medium-sized events have led to widespread devastation and caused still considerable overall insured losses."

In recent years, significant non-weather-related nat cat events, such as earthquakes or tsunamis, have been rare and, consequently, the importance of these risks has declined in the **Allianz Risk Barometer**. "Nevertheless, nat cat risks are in the top three risks in many regions across the globe that are frequently affected by meteorological, geophysical, climatological and hydrological events (e.g. US, China and Japan)," says Pfeuffer. "At the same time climate change/increasing volatility of weather is at its highest ever position in the **Allianz Risk Barometer (#7)**" (see page 19).

Download our [windstorm checklist](#)

Download our [flood checklist](#)

5

MARKET DEVELOPMENTS

(e.g. volatility, intensified competition/new entrants, M&A, market stagnation, market fluctuation)

21% ■ 2019: 5 (23%)

2019 was characterized by high market volatility, which will continue in 2020, according to **Ludovic Subran, Chief Economist at Allianz**.

Uncertainties caused by trade conflict and political risks will continue to affect markets. Low-growth-low-inflation may hide more direct pass-through from political risks to financial markets, and the need to manage negative externalities of interventionist policy-makers.

Along with rising volatility, the directionality of global markets will be hard to predict. Historically,

fixed income assets have been the outperformers in late cycle periods. A severe economic downturn would lead equity markets to a double digit downward correction. The superdovish central banks will keep bond yields at very low levels. "We expect the 10 year Bund at -0.4% at end-2020 and the 10 year U.S. yield at 1.7%," says Subran. "Higher volatility from the US-China trade conflict will keep the dollar strong. The renminbi should depreciate further. A more fragmented world also means volatile commodity prices, currencies and capital flows for emerging markets."

6

FIRE, EXPLOSION

20% ■ 2019: 6 (19%)

Fire and explosion incidents may rank as the sixth top peril for businesses in 2020 according to **Allianz Risk Barometer** respondents but it is actually the number one cause of financial losses based on the results of insurance claims analysis by AGCS. Such events have caused in excess of €14bn (\$15.7bn) worth of losses over a five-year period through 2018 – accounting for almost a quarter (24%) of the value of more than 470,000 claims examined by AGCS. This is significantly ahead of the second top cause of loss, aviation collision/crash incidents (14%). Even the average insurance claim from a fire totals almost €1.5mn (\$1.65mn).

Although fire losses for large companies have reduced with better protection and risk management, property/asset values per square meter in some industries and manufacturing sites have quadrupled over the past decade, which means that when an event does happen the cost of any damages or subsequent business interruption (fire is also the most frequent driver of business interruption claims [see page 15]) significantly increases. Even a small fire can have a large impact dollar wise, which can ripple through an entire sector. Only by assessing and maintaining a regular upkeep of fire mitigation practices onsite can companies lower the risk of loss.

¹ Swiss Re, Global catastrophes caused USD 56 billion insured losses in 2019, December 19, 2019



17% ▲ 2019: 8 (13%)

7 CLIMATE CHANGE

/increasing volatility of the weather

Companies have to consider the full spectrum of risks associated with climate change, such as the operational, reputational and regulatory impact, in addition to the potential for higher property damages from natural catastrophes. Combatting climate change requires corrective action and investment, but also brings opportunities.

Climate change/increasing volatility of weather rises to its highest-ever position in the **Allianz Risk Barometer** rankings in 2020 (17% of responses), reflecting the fact that its impact can trigger huge and unpredictable loss scenarios for business and insurers alike and therefore should be at the core of all mitigation and resilience actions. The growing cost of climate change is already noticeable. Analysis shows that the number of weather-related/flood loss events has increased by a factor of three to four since 1980.

Four years after the United Nations' momentous Paris Agreement – the target of which is to keep the increase in global average temperatures to well below 2°C above pre-industrial levels, and to try to limit the rise to 1.5°C – it has become clear that the progress and policies on emission reductions has, so far, been insufficient.

Many industries are facing major transformation risks – and expenses – in order to ensure their future business models are more climate-friendly. Overall, Allianz has estimated that responding to the challenges posed by climate change could cost companies worldwide as much as \$2.5trn

over the next 10 years¹ with the cost of making the energy sector more “green” the highest. The automotive, chemical and agriculture industries are just a few of the other sectors that will be particularly impacted.

RISKS AND OPPORTUNITIES

“If these sectors don’t prepare and take action now in a structured way they will face increasing regulatory and governmental pressure which will force them into a belated transition over a very short time period,” says **Thomas Liesch, Climate Integration Lead at Allianz**. Measures will include carbon pricing, energy and efficiency mandates, mobility regulations and industry-specific taxes, fines and levies.

Companies therefore have to address transition risks and start de-carbonizing their business models. The key to resilience is to reduce emissions and adapt to inevitable levels of climate change.

“Transformation comes with investments and costs of course, but these are outweighed by new opportunities,” says Liesch, adding that the costs

¹ Allianz, COP25 No Such Thing As A Free Lunch

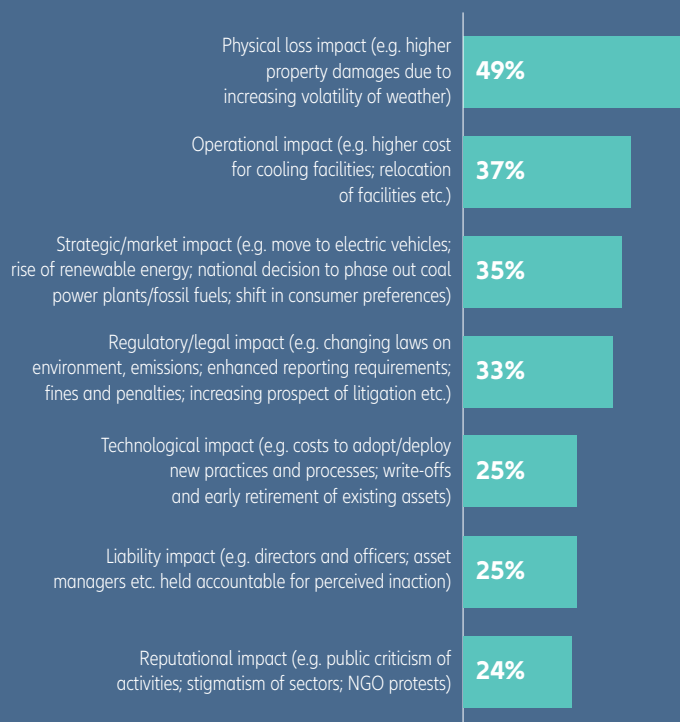
for companies can be many times lower than the business opportunities offered by new business models, products and sales markets, such as new renewable energy production methods, battery production, rare earth mining, or new technologies, such as hydrogen generation from excess renewable power, for example.

THE PHYSICAL AND HUMAN LOSS IMPACT

According to **Allianz Risk Barometer** respondents, the increase of physical losses from climate change is the exposure businesses fear most (49% of responses), followed by the operational impact and then the consequences of potential changes in their market and regulatory environments (see graphic).

2 Climate Transparency, Brown To Green, The G20 Transition Towards A Net-Zero Emissions Economy 2019

CLIMATE CHANGE: WHAT ARE THE MOST SIGNIFICANT RISK EXPOSURES ITS IMPACT CREATES FOR BUSINESSES?



“Climate change can affect businesses in many ways,” says Chris Bonnet, Head of ESG Business Services at AGCS. “Firstly, businesses face a broader range of physical loss scenarios. For example, a temperature increase of more than 2°C would expose greater parts of our world to storms and flood losses. Secondly, legal and political policies to reduce emissions are challenging industries such as automotive, transportation and utilities – they all have to transform and ‘de-carbonize’ their business models.”

Source: Allianz Global Corporate & Specialty. Figures represent the percentage of answers of all participants who responded (2,718). Figures don't add up to 100% as up to three risks could be selected.

“Economically, the physical risks and costs of a +3°C or +4°C world are many times higher than doing nothing,” says Liesch. “A significant increase in heatwaves and droughts, loss of the Amazon rainforest, desertification of the Mediterranean region, thawing of the permafrost, a rise in extreme weather events and sea-levels and a reduction in the value of exposed property, abandonment of low-lying coastal areas and increased adaption (e.g. building barriers and drainage solutions) and maintenance costs are just some of the many consequences that would lie ahead,” Liesch notes, citing the findings of **The Heat Is On – Insurability and Resilience In A Changing Climate** report by the CRO Forum, a group of professional risk managers from the insurance industry, of which Allianz is a member.

Global warming fuels extreme calamities worldwide and threatens business. Rising seas, drier droughts, fiercer storms and massive flooding pose physical threats to firms because they imperil factories and other assets, as well as transport and energy links that tie the entire supply chain together.

“Climate change is often presented as an issue for tomorrow with global warming paths calculated for the end of the century. But this perspective is swiftly changing,” says **Amer Ahmed, CEO of Allianz SE Reinsurance**. “A focus in public discourse on a ‘climate crisis’ or ‘climate emergency’ is emphasizing the toll our society is already paying today.”

Allianz Re provides an annual award to researchers into climate change, as well as solutions to mitigate the effects. “As risk-carriers, insurers have skin in the game,” says Ahmed. “And the climate crisis is already impacting our business.”

For example, 2017 was a year of particularly significant catastrophes. Houston experienced its third “500-year flood” in less than four decades, while California suffered five of its 20 most destructive wildfires ever.

Meanwhile, 41 million people in Bangladesh, India and Nepal were affected by flooding and monsoon rains. Conversely, commercial traffic on the Rhine, the world’s busiest waterway, was stranded when waters reached a historic low.

Events such as these have a heart-wrenching human cost and not just in the poorest countries either. According to a recent report from Climate Transparency, there are 16,000 fatalities in G20 economies due to extreme weather events every year. The economic impact is estimated to be \$142bn annually².

INCREASING REGULATORY, INVESTOR AND LIABILITY THREATS

There are a growing number of other perils associated with climate change that need to be addressed in both developed jurisdictions and emerging markets in addition to companies facing the prospect of larger losses from more severe weather events.

“Companies are realizing that they may face consumer criticism, reputational damage and increasing regulatory and legal action if they don’t adequately address climate change in their business strategy, operations and product offerings,” says **Chris Bonnet, Head of ESG Business Services at AGCS.**

It is estimated that around 1,500 new laws are being introduced around the world every year in response to climate change, although different jurisdictions are taking different approaches.

Europe is focused on the financial sector – for example, in the UK, it was recently announced that lenders and insurers will be tested against three different scenarios that stretch out decades under what the Bank of England claims will be the “world’s stiffest climate stress tests”. In Australia, there has been a lot of work to integrate climate risk into prudential regulations. Japan has recognized that the integrated nature of its financial system and heavy industry calls for a joined-up approach – 194 companies have adopted the recommendations of the Task Force On Climate-Related Financial Disclosures. Singapore is also regarded as one of the leaders when it comes to climate change disclosure.

It is not just governments and regulators who are putting pressure on companies about how they are responding to climate change, however. Climate-linked activism against corporates is a developing trend – particularly in Europe – and boards are increasingly being challenged by investors and other stakeholders. For example, activist hedge fund TCI recently outlined plans to punish directors of companies that fail to disclose their carbon dioxide emissions and also called on asset owners to fire fund managers that do not insist on climate transparency³.

“Many stakeholders have an interest in corporates’ response to climate risk, and any reputational damage from failure to take action will influence stakeholder choices,” says **Karsten Berlage, Regional Head, Americas, at AGCS’ Alternative Risk Transfer unit.** “Capital investors may choose against a firm deemed not to be environmentally-friendly, while ratings agencies



Failure to disclose climate change risk will drive more litigation in future

and the media will be looking closely at what companies are doing to avoid climate disasters.”

There is little doubt that a failure to disclose climate change risk will drive more litigation in future years. Climate change cases have already been brought in around 30 countries around the world to date with three-quarters of those cases filed in the US. In the US, there are an increasing number of cases alleging that companies have failed to adjust business practices in line with changing climate conditions. Many lawsuits are currently targeting the so-called “carbon majors” – active fossil fuel producers. However, this will likely expand to other carbon-heavy industries, such as agri-business, manufacturing and transport.

PREPARING FOR THE FUTURE

“Given directors could be held responsible for how environmental, social and governance (ESG) issues and climate change are addressed at a corporate level, they will have to consider the impact of these when looking at strategy, governance, risk management and financial reporting,” says **Shanil Williams, Global Head of Financial Lines, AGCS.** “Preparing a company’s business model for a low-carbon future is a multi-departmental approach involving strategy, governance and reporting, risk management and business-facing functions.”

“Every company has to define its role and pace in the climate change transition and develop a clear stance involving and addressing key stakeholders,” adds Bonnet. “Risk managers need to drive ESG and climate change focus internally to influence decisions.

“Many companies today focus on risk reporting rather than risk management. To understand the real impact of climate changes you have to look beyond the usual two-to five-year time horizon and anticipate and prepare for various future scenarios.”

³ Financial Times, Hedge fund TCI vows to punish directors over climate change, December 2019

8

LOSS OF REPUTATION OR BRAND VALUE

15% ▲ 2019: 9 (13%)

Corporate scandals involving reputation can originate from an increasing number of scenarios – from cyber breaches to social media to corporate misconduct to even supplier misconduct. Calculating the value of a company’s reputation can be difficult but when bad news comes – and a company suffers a blow to its reputation its value becomes obvious – market value can collapse with astonishing speed. It is estimated that more than one quarter of reputational crises spread within an hour and over two-thirds within 24 hours. The impact of reputation events on stock prices is believed to have doubled since the introduction of social media.

Despite the growing risks, many companies are still inadequately protected against the consequences of a reputational crisis. Effective planning and crisis management have become essential and a professional response can make a difference. Research shows that the value of a company that effectively manages a reputational crisis can rise by 6% the following year.

Increasingly, insurance can also provide tangible assistance to an intangible risk, providing solutions such as protection against reduced net operating profit related to a reputational event, rectification advice costs, a 24/7 reputational crisis response and strategic media analysis reports.

➤ [For more information on reputational risk insurance](#)

9

NEW TECHNOLOGIES

(e.g. impact of Artificial Intelligence, autonomous vehicles, 3D printing, Internet of Things, nanotechnology, blockchain)

13% ▼ 2019: 7 (19%)

New technologies present considerable opportunities for businesses. However, they can also bring risks, sometimes with unintended consequences. According to **Allianz Risk Barometer** respondents, the increasing utilization

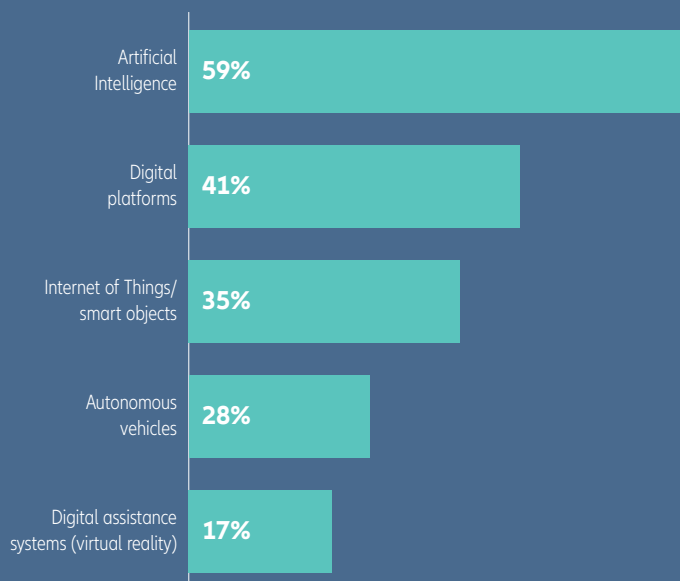
of Artificial Intelligence (AI), which is an important driver of change in many industries today, is the new technology that also comes with the greatest future risk potential (see chart left).

“From chatbots to autonomous cars, more widespread implementation of AI applications is transforming industry and society, bringing benefits such as increased efficiencies, new products and less repetitive tasks,” explains **Michael Bruch, Global Head of Liability Risk Consulting/ESG at AGCS**.

“For example, in the insurance industry, AI applications will improve the transaction process, with many benefits already apparent. Customer needs can be better identified. Policies can be issued, and claims processed more quickly and cheaply. Large corporate risks, such as business interruptions, cyber security threats or macro-economic crises, can be better predicted. Meanwhile, chatbots can assist customers on a 24/7 basis.”

However, with progress in AI, machines may begin to make decisions on behalf of humans. Decision transfer and lack of transparency or human oversight may result in unforeseen risks or unpredictable outcomes creating complex liability issues. At the same time, ethical and social concerns related to AI are also becoming more prominent, says Bruch.

WHICH OF THESE EMERGING TRENDS COMES WITH THE GREATEST RISK POTENTIAL IN THE NEXT FIVE TO 10 YEARS?



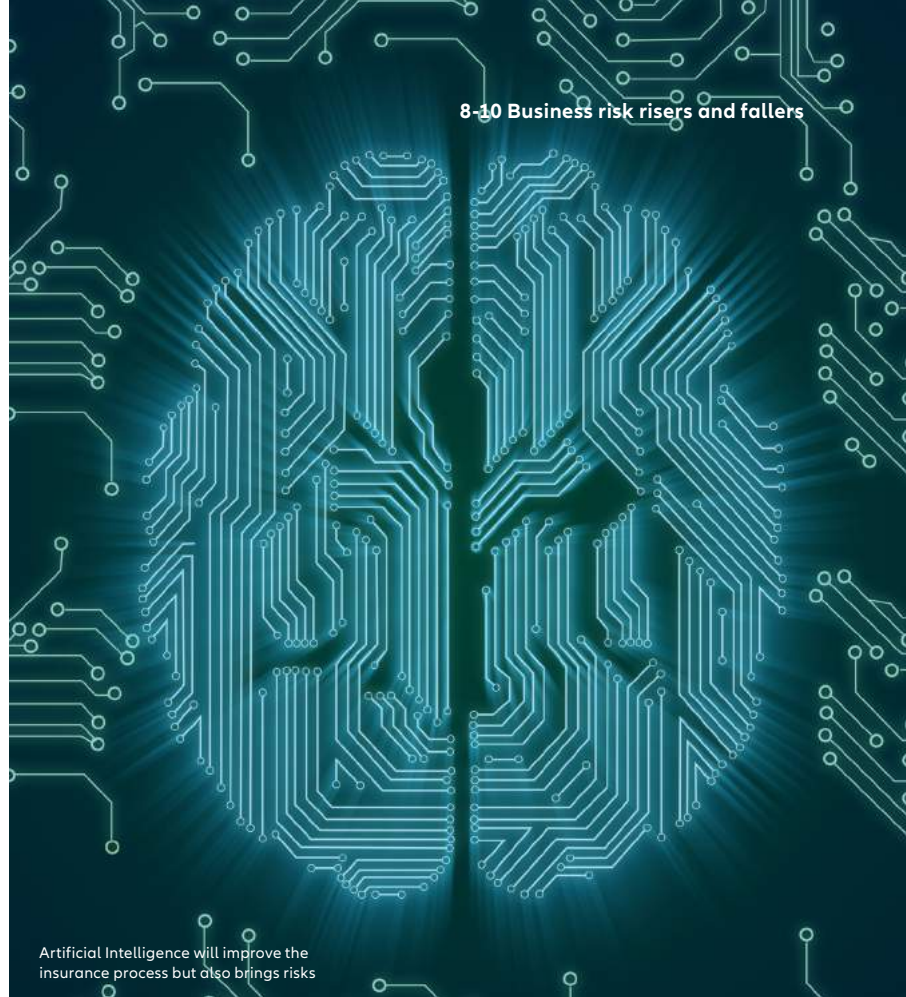
Source: Allianz Global Corporate & Specialty. Figures represent the percentage of answers of all participants who responded (2,718). Figures don't add up to 100% as up to three risks could be selected.

DIGITAL PLATFORMS DOMINATE

Of all the complex technological developments confronting companies today, the one with the most immediate impact is digital platforms. The collection of cloud-based software and services used to drive business have developed over the last decade as firms have built on, or moved core functions on to, digital platforms. This trend has now reached critical mass, according to the **AGCS Trend Compass**, a report which identifies the most important technological, business and socio-economic developments of the future.

Such platforms enable the direct digital interaction of two or more user sites, bringing together communities of buyers and sellers so goods, information, jobs and services can be freely offered or requested. This creates markets of enormous scale – seven out of the 10 most valuable companies globally are based on a platform business model. However, growing reliance on digital platforms also brings greater risk potential, according to **Allianz Risk Barometer** respondents, ranking second behind AI in this regard.

“There are a number of risks for those large corporates who are being confronted by the rise of platforms in their respective industries,” says **Adeline Roupillard, Global Practice Head of Digital Transformation at AGCS**. “Platforms can lead to a monopoly game – early platforms have come to dominate entire markets by redefining how participants interacted. In other industries, where platforms have not emerged as quickly, companies cannot afford competitor’s platforms to become the standard because then they will be tethered and pay a significant cost to do business. If as a company you do not run and lead the industry platform, you also run the risk of slowly losing your direct



access to the clients and the valuable data resulting from the client relationship which can damage your brand.”

And as digital platforms become bigger and bigger, interconnectivity becomes an increasing risk. If one element breaks it can have an impact on a whole value chain, such as a business interruption cascading through an entire sector if a platform is unavailable due to a technical glitch or cyber event. The losses from such an event for multiple companies could be in the hundreds or even billions of dollars if any outage lasts for a significant amount of time.

[Find out more about Artificial Intelligence risks](#)

10

MACROECONOMIC DEVELOPMENTS

11% ▲ NEW

(e.g. monetary policies, austerity programs, commodity price increase, deflation, inflation)

In the course of 2019, recession risks became more and more visible. In 2019-20, superdovish central bankers, and a new fiscal impulse (US, China and Europe, to a lesser extent) will help avoid a global recession, according to **Ludovic Subran, Chief Economist at Allianz**. However, flatlining growth will be the norm.

Over the summer of 2019, escalating political risks (US-China rivalry, Brexit, a new government in Italy) exacerbated the pockets of recession visible in the first half of the year in trade,

manufacturing and a dozen of economies.

“Looking ahead, a soft landing remains our baseline scenario,” says Subran. “Consumers will be a source of resilience. While monetary stimulus has worked well in the past, we believe it will be increasingly ineffective at current rates while it will feed into higher vulnerabilities. Debt accumulation, from already high levels, could start to be a cause of worry in the US and China, notably with regards to the private sector, and in the case of a too-fast-and-badly-managed exit from such accommodative monetary policies.”

CONTACT US

For more information contact your local Allianz Global Corporate & Specialty Communications team.

Africa

Lesiba Sethoga
lesiba.sethoga@allianz.com
+27 11 214 7948

Asia Pacific

Wendy Koh
wendy.koh@allianz.com
+65 6395 3796

Central and Eastern Europe

Daniel Aschoff
daniel.aschoff@allianz.com
+49 89 3800 18900

Mediterranean

Florence Claret
florence.claret@allianz.com
+33 158 858863

North America

Sabrina Glavan
sabrina.glavan@agcs.allianz.com
+1 646 472 1510

South America

Camila Corsini
camila.corsini@allianz.com
+55 11 3527 0235

UK, Middle East, Nordics

Jonathan Tilburn
jonathan.tilburn@allianz.com
+44 20 3451 3128

Global

Hugo Kidston
hugo.kidston@allianz.com
+44 203 451 3891

Heidi Polke-Markmann
heidi.polke@allianz.com
+49 89 3800 14303

Editorial Team: Greg Dobie, Christina Hubmann, Damien Keg, Alejandra Larumbe, Heidi Polke and Joel Whitehead.

Design: Kapusniak Design

For more information contact
agcs.communication@allianz.com

Follow Allianz Global Corporate & Specialty on



Twitter [@AGCS_Insurance](#) [#ARB2020](#) and



LinkedIn

www.agcs.allianz.com

[Download the full Allianz Risk Barometer 2020 results](#)

Disclaimer & Copyright

Copyright © 2020 Allianz Global Corporate & Specialty SE. All rights reserved.

The material contained in this publication is designed to provide general information only. Whilst 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 Allianz Global Corporate & Specialty SE cannot be held responsible for any mistakes or omissions.

Allianz Global Corporate & Specialty SE
Fritz-Schaeffer-Strasse 9, 81737 Munich, Germany
Commercial Register: Munch HRB 208312

Images: Adobe Stock/iStockPhoto

January 2020