ALLIANZ RISK BAROMETER

TOP BUSINESS RISKS FOR 2019

The most important corporate perils for the year ahead and beyond, based on the insight of more than 2,400 risk management experts from over 80 countries

Allianz

About Allianz Global Corporate & Specialty

Allianz Global Corporate & Specialty (AGCS) is the Allianz Group's dedicated carrier for corporate and specialty insurance business. AGCS provides insurance and risk consultancy across the whole spectrum of specialty, alternative risk transfer and corporate business.

- Alternative Risk Transfer
- Aviation (including space)
- Energy
- Engineering
- Entertainment
- Financial Lines (including Directors and Officers)
- Liability
- Marine
- Mid-Corporate
- Property (including International Insurance Programs)

Worldwide, AGCS operates with its own teams in 34 countries and through the Allianz Group network and partners in over 210 countries and territories, employing almost 4,700 people of 70 nationalities.

AGCS provides insurance solutions to more than three quarters of the **Fortune Global 500** companies, writing a total of €7.4bn gross premium worldwide in 2017.

AGCS SE is rated AA by Standard & Poor's and A+ by AM Best

ALLIANZ RISK BAROMETER METHODOLOGY

The eighth **Allianz Risk Barometer** is the biggest yet incorporating the views of a record 2,415 respondents from 86 countries. 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 2018. The survey focused on large and small- to mid-sized enterprises. Respondents were asked to select industries about which they were particularly knowledgeable and name up to three risks they believed to be of the most importance. Applicable respondents could provide answers for up to two industries meaning there was a total of 2,882 survey responses from 2,415 respondents.

Most answers were for large enterprises (>€500mn annual revenue) [1,445 responses 50%]. Mid-sized enterprises (€250mn to €500mn revenue) contributed 619 responses (21%), while small enterprises (<€250mn revenue) produced 818 responses (28%). 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**

2,415
respondents

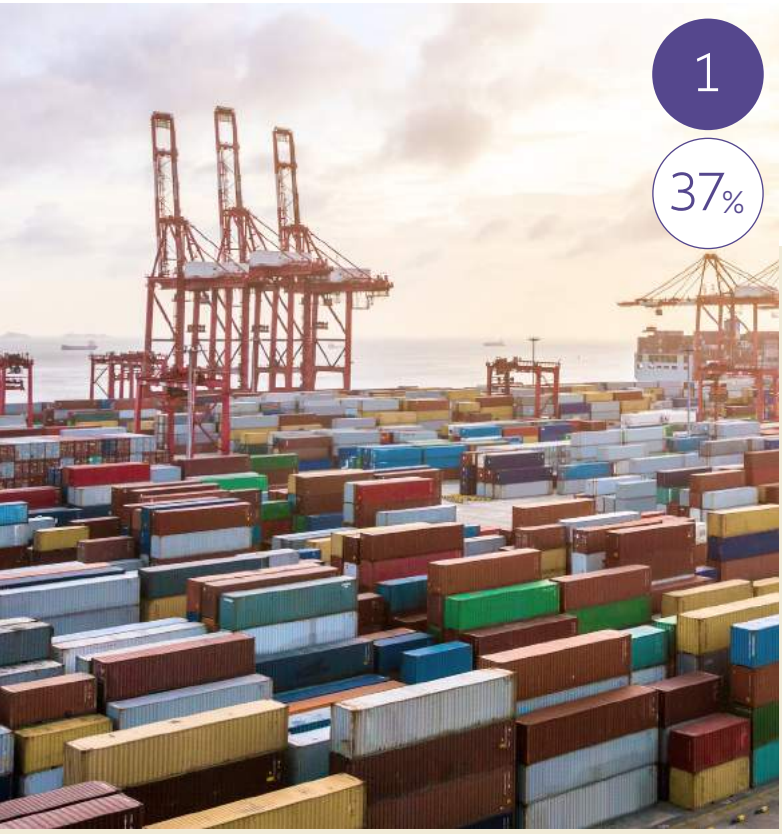
86
countries

2,882
responses

22
industry sectors

CONTENTS

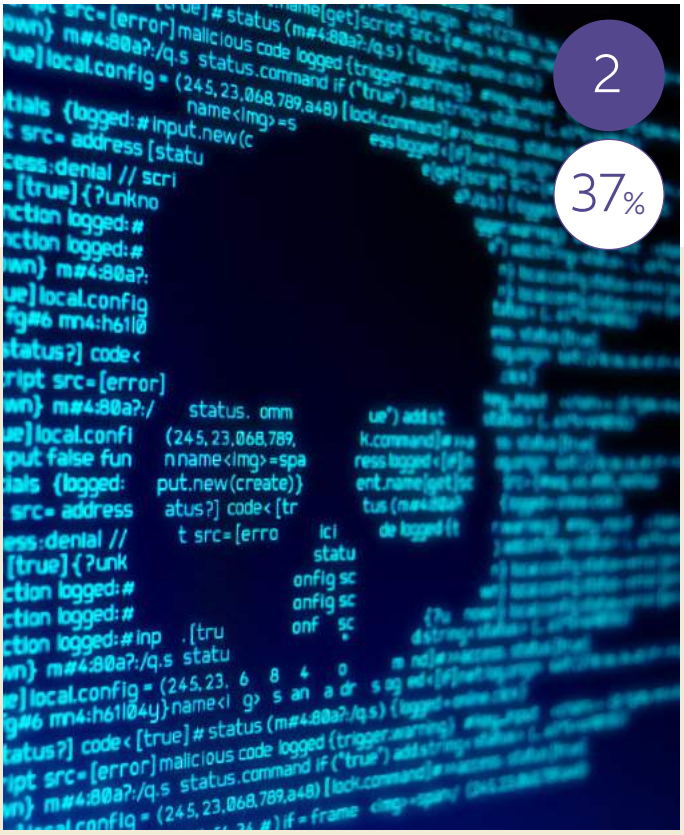
Source: Allianz Global Corporate & Specialty.
Figures represent the number of risks selected as a percentage of all survey responses (2,882) from 2,415 respondents. Applicable respondents could provide answers for up to two industries. All respondents could select up to three risks per industry.
Ranking changes in the Allianz Risk Barometer are determined by positions year-on-year not percentages.



(=) 2018: 1 (42%)

Business interruption

(incl. supply chain disruption)



(=) 2018: 2 (40%)

Cyber incidents[1]

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

1 **Business interruption and cyber incidents are tied at the top of the ranking at 37%. However, business interruption received more responses by number**

2 Fire, explosion ranks higher than new technologies by number of responses

3 Climate change/increasing volatility of weather ranks higher than loss of reputation or brand value by number of responses

KEY

Risk higher than in 2018

Risk lower than in 2018

No change in 2018

1 **2018 risk ranking**

(=) 2018: 6 (20%)

Fire, explosion

(=) 2018: 7 (15%)

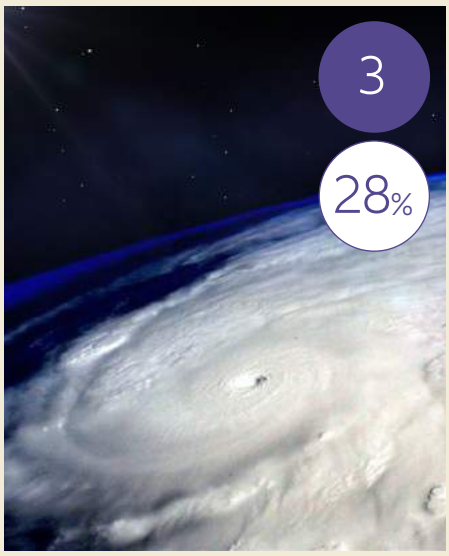
New technologies[2]

(e.g. impact of increasing interconnectivity, nanotechnology, artificial intelligence, 3D printing, autonomous vehicles, blockchain)

ALLIANZ RISK BAROMETER

TOP 10 GLOBAL BUSINESS RISKS FOR 2019

↘ View the full Risk Barometer 2019 rankings here



(=) 2018: 3 (30%)

Natural catastrophes
(e.g. storm, flood, earthquake)

(▲) 2018: 5 (21%)

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

(▼) 2018: 4 (22%)

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

(▲) 2018: 10 (10%)

Climate change/ increasing volatility of weather

(▼) 2018: 8 (13%)

Loss of reputation or brand value[3]

(▲) NEW

Shortage of skilled workforce

SNAPSHOT: TOP BUSINESS RISKS AROUND THE WORLD IN 2019

USA
"It's telling that business interruption (BI) has surpassed cyber incidents as the foremost business risk in the US. This validates the magnitude by which today's risk managers face challenging traditional and emerging exposures that can leave their companies highly vulnerable. Last year's report had the two in reverse order, showing the continued heightened focus on both risks and how they remain increasingly interlinked disrupters."
BILL SCALDAFERRI, PRESIDENT & CEO, AGCS NORTH AMERICA

Brazil
"Cyber incidents have consolidated first place in the Brazil rankings, reflecting the growing exposure of companies to e-commerce and digitalization of financial transactions."
ANGELO COLOMBO, CEO, AGCS SOUTH AMERICA

UK
"It's no surprise to see changes in legislation and regulation as the new top risk in the UK, jointly with cyber-attacks. Uncertainty around Brexit, along with the increase in the regulatory burden and global trade disputes, has made confidence fragile. UK businesses also continue to be occupied by the threat of cyber-attacks."
TRACEY HUNT, DEPUTY CEO, AGCS UK

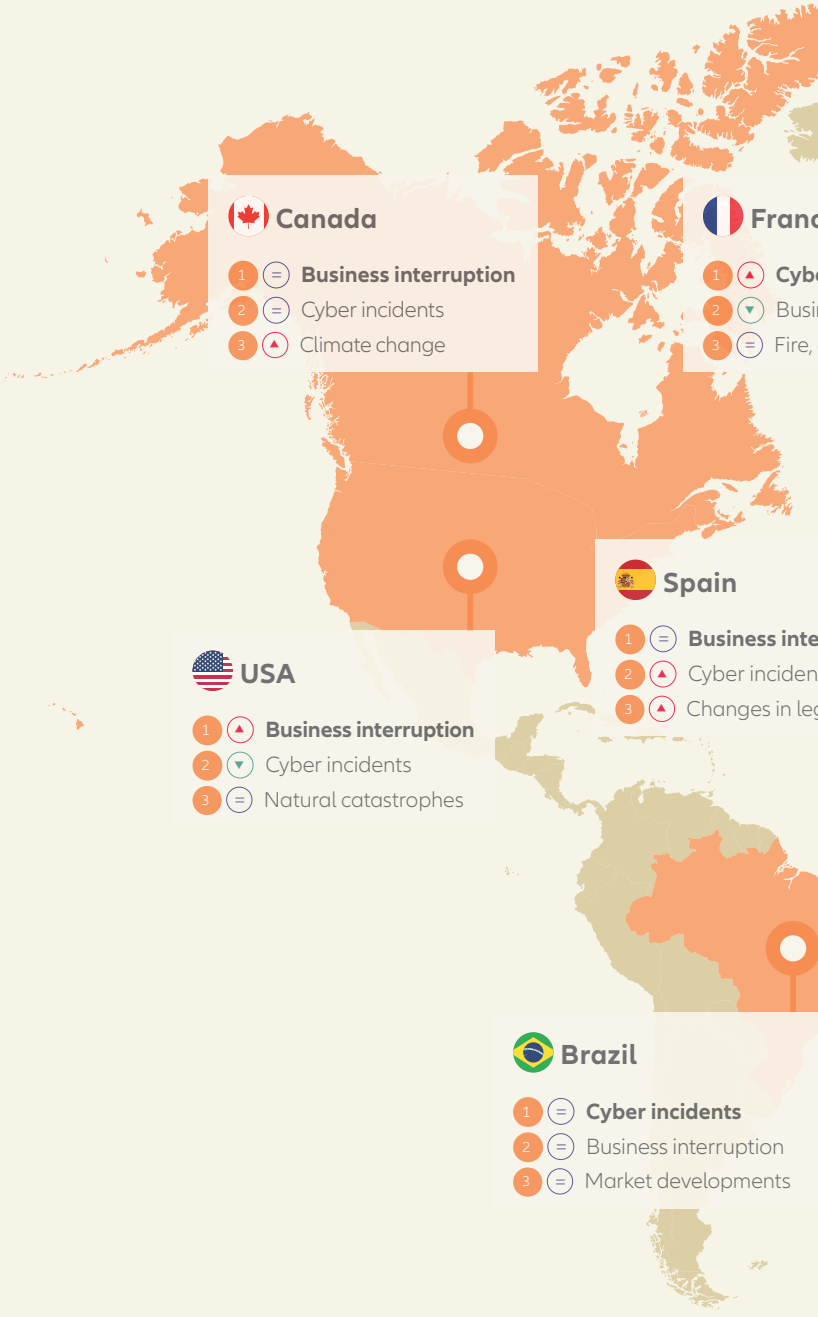
Canada
"Regulatory and legislative changes continue to impact the Canada risk outlook, including new privacy breach reporting obligations. Climate change and natural catastrophes remain in the Top 10, joined by environmental risks. Such threats include pollution exposures caused by natural catastrophes leading to BI. The demand for insurance solutions for both these risks, including contingent BI, is on the rise."
ULRICH KADOW, CEO, AGCS CANADA

Germany
"Cyber risks and BI are the biggest threats to German businesses. As cyber incidents are increasingly the cause of BI, both risks have become more intertwined. Ransomware attacks such as NotPetya and WannaCry have led to large-scale disruptions at companies and caused large losses worldwide. Increasing connectivity and common IT infrastructure makes all links in the supply chain susceptible to cyber incidents. To effectively deal with these twin evils is therefore not an option, but an obligation for risk managers and insurers."
CHRIS FISCHER HIRS, CEO, AGCS

France
"French businesses are more and more concerned by the increasing frequency and severity of cyber incidents, making cyber the top risk for the first time ever in France."
CORINNE CIPIÈRE, CEO, AGCS FRANCE

Italy
"Following a recent rise in the number of food recalls, product recall becomes a notable new entry in the rankings in Italy (4th)."
NICOLA MANCINO, CEO, AGCS ITALY

Spain
"Recent cyber-attacks to important local institutions explain the rapid rise of cyber incidents in Spain, moving up from 4th to 2nd position year-on-year."
JUAN MANUEL NEGRO, CEO, AGCS SPAIN



Asia Pacific
"Businesses across Asia Pacific are deeply concerned about the impact of BI. The average BI property insurance claim is now over €3mn. As manufacturing shifts east, and with growing frequency of natural catastrophe activity in the region, Asia Pacific is increasingly exposed to these losses reflecting the importance for companies to adopt a holistic approach to risk management."
MARK MITCHELL, CEO, AGCS ASIA PACIFIC

This risk map shows the top three risks for businesses in **selected countries**.
Source: Allianz Global Corporate & Specialty

↘ View all country, regional and industry risk data here

Africa

"Businesses in Africa are faced with political instability and policy uncertainty, which are among the key risk factors that have an impact on business/investor confidence. For Africa to stay globally competitive, companies needs to be at the cutting edge of technological advancement, yet new technologies can also bring cyber incidents. It is vital that companies mitigate against risks through modern risk management methods and trusted insurance solutions."

THUSANG MAHLANGU, CEO, AGCS AFRICA

KEY

▲ **Risk higher than in 2018**

▼ **Risk lower than in 2018**

= **No change from 2018**

EXECUTIVE SUMMARY

Technology is breeding new threats as well as business models. Traditional risks such as natural catastrophes continue to challenge while other threats such as cyber, neck-and-neck with business interruption at the top of the Allianz Risk Barometer for the first time, reputational risk, increasing exposure to intangible assets and volatility and consolidation in the corporate environment evolve daily.

A consequence of many of the other top risks in the Allianz Risk Barometer, **business interruption (BI)** is the top threat for companies for the seventh year running (37% of responses). According to AGCS, the average BI property insurance claim now totals over €3mn ($3.4mn) at €3.1mn. This is more than a third (39%) higher than the corresponding average direct property damage loss (€2.2mn) with these totals significantly higher than five years ago. Losses from the largest events can be in the hundreds of millions or higher.

Businesses face an increasing number of BI scenarios. Many can occur without physical damage but with high losses. Events such as breakdown of core IT systems, product recall or quality incidents, terrorism, political violence or rioting and environmental pollution can bring businesses to a standstill, meaning firms may be unable to provide products and services – or customers stay away – having a devastating effect on revenues. For example, retailers lost about €1bn ($1.1bn) from four weekends of protests in France at the end of 2018.[1] In today's uncertain political landscape, legislative change such as the UK's expected Brexit departure from the European Union in 2019 also poses a potential BI threat with supply chain disruption anticipated. ↘ Page 10

BI is joined at the top of the ranking for the first time by **cyber incidents** (37%)[2]. According to AGCS, even the average insured loss from a cyber incident is now just over €2mn[3] ($2.3mn) compared with almost €1.5mn from a fire/explosion incident, while losses from major events can be in the hundreds of millions or higher. Increasingly, cyber incidents bring their own BI losses. Respondents rank cyber as the BI trigger they fear most, given many companies' primary assets can often be data, service platforms or groups of customers or suppliers.

BI loss was a hallmark of the **WannaCry** and **NotPetya** malware attacks in 2017 which disrupted shipping, logistics and manufacturing companies. Insurers have seen a growing number of BI losses trigged by cyber incidents with industry claims exceeding $100mn.

Many incidents are the result of technical glitches or human error rather than malicious acts – analysis conducted by the UK's financial services regulator revealed a 138% increase in technology outages over a year but just 18% of reported incidents were cyber-attacks.[4]

IT outages pose a significant risk. Incidents such as power surges or failed IT platform migrations can cost hundreds of millions. Reliance on IT service providers – such as cloud services, online booking platforms and supply chain systems – also brings potential contingent business interruption (CBI) exposures. A software glitch at network equipment provider Ericsson disrupted services for millions of mobile phone customers in Europe and Japan in 2018[5]. In 2017, a four hour outage at Amazon's AWS cloud computing division impacted internet services, websites and

1 BBC News, Yellow vest protests 'economic catastrophe' for France, December 9, 2018

2 BI and cyber incidents tied on 37%. BI received more responses by number – 1,078 to 1,052.

3 Average value of cyber claim is €2,007,653 based on 115 insurance industry claims between 2013 and 2018.

4 The Financial Conduct Authority, Cyber and technology resilience in UK financial services, November 27, 2018

5 Reuters, Ericsson sorry for software glitch that hits mobile services in Britain and Japan, December 6, 2018

other businesses. Companies lost approximately $150mn as a result[6]. Longer outages could see losses much closer to a billion dollars. ↘ Page 14

Increasing concern over cyber incidents follows a watershed year of activity. Cyber crime costs an estimated $600bn a year[7] up from $445bn in 2014. This compares with a 10-year average economic loss from natural catastrophes of around $200bn – three times as much. There is also a growing threat from nation states, which use technology to steal valuable data and trade secrets, with implications for businesses.

Impact of mega data breaches, privacy scandals and the introduction of the European Union's General Data Protection Regulation – which has also inspired tougher privacy rules and the threat of large fines elsewhere – are also occupying companies' thoughts. Cyber incidents are increasingly likely to spark litigation, including securities and consumer class actions. ↘ Page 12

Every company needs to adopt an IT security position which is adequate to its size, operations and risk profile and invest in technological security solutions, proper backup mechanisms and staff training. The last aspect is equally important, especially for small and mid-sized enterprises, for which awareness of the growing cyber threat and its link to loss of reputation is a growing concern. ↘ Page 22

Major events such as hurricanes Michael and Florence in North America, Typhoon Jebi in Japan and more wildfires in California brought approximately $146bn[8] of economic losses from **natural catastrophes** (3rd 28%) in 2018 coming on the back of a record loss year in 2017. Respondents are concerned that recent activity could be a harbinger of increasing financial losses and disruption ensuring **climate change** (8th 13%) rises to its highest-ever position. In addition to damage and disruption to property, climate change is likely to have big implications for regulation and liability. Emissions targets are already shaping industries like aviation and shipping. Growing reporting and disclosure requirements will increase exposures for companies and directors and officers.
↘ Pages 16 and 20

Businesses are more concerned about **changes in legislation and regulation** (4th 27%) than 12 months ago with trade wars, tariffs and ongoing uncertainty over **Brexit** heightening fears about the resilience of supply chains. **Market developments** (5th 23%) remains a top five risk after 2018 was marked by record volatility, divergence and surprises, with more of the same expected in 2019. Impact of **fire, explosion** incidents (6th 19%) is a perennial concern. According to AGCS, fires (not including wildfires) have caused in excess of €14bn ($15.9bn) worth of insurance losses over the past five years, making it the top cause of loss for businesses.

New technologies (7th 19%)[9] present fantastic opportunities for business, including new ways to manage risk. However, as the number of connected machines increases it also brings questions around security, data protection, business continuity and third party liability, as well as the potential for critical infrastructure breakdown. Unexpected consequences continue to materialize, such as drone activity cancelling some 1,000 aircraft at the UK's Gatwick airport in December 2018. Meanwhile, product recalls, cyber incidents and executive conduct have all tainted the reputations of organizations in recent years, affecting airlines, car manufacturers, banks and charities meaning protecting against **loss of reputation or brand value** (9th 13%) takes on urgency in the social media age when crises spread rapidly. **Shortage of skilled workforce** (10th 9%) appears in the top 10 global risks for the first time with factors such as changing demographics, and Brexit contributing to its rise.
↘ Page 18

Such a long and diverse list of threats requires new risk management solutions, tools and partnerships to manage and mitigate its potential impacts. Insurance is increasingly providing tangible assistance to intangible risks. Cyber insurance is becoming a valuable part of incident response by providing companies access to specialist consulting services which can help battle and better prepare for events. Cyber BI insurance can defend against loss of income and costs from unavailability of data and systems caused by hacking, technical failure or employee error. Non-damage BI insurance indemnifies a business for revenue loss from a disruptive event such as a protest or riot. Reputational risk insurance provides advisory and response costs in event of crisis.

New technologies are also boosting risk analysis. Insurers such as AGCS now utilize semantics analysis to better understand supply chain risk, drones to quickly assess catastrophe damage and are partnering with insurtechs to identify next generation litigation risks. In an increasingly networked world, data from devices, factories and supply chains will provide an opportunity for even better risk assessment through predictive indicators and more flexible, tailored and timely solutions, with the ultimate aim being to understand and manage risks more quickly in order to prevent losses before they occur.

6 Guidewire Cyence Risk Analytics, MMC Cyber Handbook 2018, Evolution of Cyber Risks Quantifying Systemic Exposures

7 Center for Strategic and International Studies, Economic Impact of Cybercrime – No Slowing Down

8 Swiss Re, December 18, 2018

9 Fire, explosion and new technologies tied at 19%. Fire, explosion received more responses

(=) 2019: 1 (37%)

1 MAJOR RISKS IN FOCUS
BUSINESS INTERRUPTION

From product recalls to riots to environmental incidents to Brexit the evolving nature of risk, and rise in cyber-related incidents, means business interruption continues to rank as a top threat globally.

5-year risk ranking (% of responses and position):
2018: 1 (42%)
2017: 1 (37%)
2016: 1 (38%)
2015: 1 (46%)

Top risk in:
- Canada
- China
- Germany
- Italy
- Netherlands
- Poland
- Portugal
- Russia
- Singapore
- South Africa
- South Korea
- Spain
- Switzerland
- USA

Top risk in the following sectors:
- Chemicals
- Consumer Goods
- Food & Beverages
- Heavy Industry
- Hospitality, Leisure, Tourism
- Manufacturing (incl. Automotive)
- Mining
- Oil & Gas
- Power & Utilities
- Renewable Energy
- Retailing, Wholesale

Impact of **business interruption (incl. supply change disruption)** is the major risk for companies for the seventh year in a row according to the Allianz Risk Barometer with 37% of responses ranking it as one of the three most important risks companies face in 2019. Fittingly, it is joined at the top of the rankings for the first time by **cyber incidents (e.g. cyber crime, IT failure/outage, data breaches, fines and penalties)** (37%)[1] which are increasingly resulting in significant business interruption (BI) losses of their own *(see page 14)*.

"Cyber incidents can cripple a company's operations and severely impair its ability to deliver its services, yet they are just one of many loss triggers that can result in a BI for corporates," says **Volker Muench, Global Practice Leader, Utilities & Services, IT Communication, AGCS**. *"BI can be a consequence of many of the other top risks in this year's Allianz Risk Barometer."*

Irrespective of whether it results from traditional exposures such as a fire at a manufacturing plant or a natural catastrophe which impacts production, a break in the supply chain due to property damages at the premises of a supplier or customer (often known as contingent business interruption [CBI]) or even a riot or civil unrest, BI can have a tremendous effect on a company's revenues, even if the event occurred thousands of miles away. And its impact can be one of the hardest risks to measure.

Claims analysis from AGCS highlights the growing relevance of BI as a consequence of losses in property insurance, heightened by today's increasingly interconnected and globalized business environment. Almost all large property insurance claims now include a major BI element, which typically accounts for the majority of the loss when previously the split might have been nearer to 50:50. The average BI property insurance claim

WHICH CAUSES OF BUSINESS INTERRUPTION (BI) DO BUSINESSES FEAR THE IMPACT OF MOST?

1. Cyber incidents
2. Fire, explosion
3. Natural catastrophes
4. Supplier failure, lean processes
5. Machinery breakdown[1]

Source: Allianz Global Corporate & Specialty. Figures represent the percentage of answers of all participants who responded (947). Figures don't add up to 100% as up to three risks could be selected.

1 Supplier failure ranks higher than machinery breakdown by number of responses

Cyber incidents ranks as the most feared BI trigger for business. Events such as the WannaCry and Petya ransomware attacks and other recent incidents are increasingly bringing significant disruption and financial losses to businesses. Yet technical failures or employee error are also frequent causes of cyber BI *(see page 14)*.

BI and CBI losses are becoming larger and more complex as supply chains become leaner with greater concentration on a smaller number of suppliers, particularly in industries like automotive, electronics and pharmaceuticals. An event such as a small fire in these industries can bring huge losses.

"Today, a single fire event at a small supplier can cause significant supply chain interruptions in the automotive industry, leading to a shortage of parts, for example," says **Volker Muench, Global Practice Leader, Utilities & Services, IT Communication, AGCS**. *"We have seen insurance industry losses from such events in excess of €1bn ($1.1bn). With one fire, a plant can go down, manufacturing has to stop and supply chain losses are subsequently generated. Machinery breakdown can have a similar effect."*

now totals over €3mn ($3.4mn) at €3.1mn. This is more than a third (39%) higher than the corresponding average direct property damage loss (€2.2mn)[2] with both of these totals now significantly higher than five years ago.

BI THREATS CONTINUE TO EVOLVE

Moreover, businesses are facing an increasing number of disruptive BI scenarios as the nature of the risk evolves in today's networked society. Many of these scenarios can occur without physical damage but with high financial losses. Breakdown of core IT systems *(see page 14)*, product recall or quality incidents, terrorism and political violence events or riots, environmental or pollution incidents or even regulatory change can bring businesses to a temporary or prolonged standstill and have a devastating effect on revenues.

Product recall and quality incidents pose an increasing BI threat, says Muench. *"We see these kinds of issues increasing. If one product at the beginning of the supply chain is not the correct one it can affect the whole process and the final product. This frequently happens in the automotive industry, for example."*

Political risk, violence and commotion events are also happening more often than in the past, says Muench, and the indirect impact of such incidents can result in BI and loss of income either from production having to be halted or customers staying away from affected areas. The fall-out from events such as rioting and protesting in France during November and December 2018 can be costly. For example, the French retail federation told Reuters news agency that retailers had lost about €1bn ($1.1bn) since the protests first began on November 17[3].

BI can also emerge when companies experience environmental issues such as pollution happening at a manufacturing site, on residential real estate or through pipeline spills. This is an often overlooked BI exposure. Expenses and supply chain disruption can quickly grow as a result of lengthy remediation, reconstruction and delays during which firms may be unable to operate or provide products or services.

Meanwhile, in today's uncertain political and business landscape, changes in regulation and legislation, such as the UK's expected Brexit departure from the EU at the end of March 2019, also bring significant BI risk.

"Supply chain disruption could be caused by the closing of borders," says Muench. *"If a manufacturing company needs a part or component from the UK or UK companies need parts or components from different countries this process could take longer than previously."*

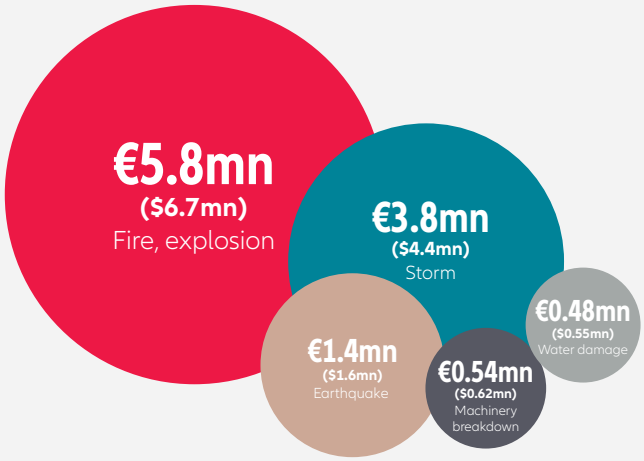
For example, there have already been reports that the UK is running out of food warehousing space as retailers and manufacturers rush to stockpile amid fears of a no-deal Brexit[4]. Frozen and chilled food warehouses are fully booked for six months, with customers being turned away, due to fears the supply chain will be interrupted after the UK's planned departure from the EU.

PLANNING FOR BI

BI risk can be physical, virtual, reputational and always financial – and therefore should be well-planned for. Companies can often underestimate the complexity of getting back to business but risks can be mitigated. A sound business continuity plan should be written and tested in a tabletop exercise to be effective. Ideally, the tabletop exercise should be prepared well in advance and designed to test location-specific vulnerabilities.

Insurers such as AGCS support businesses further though provision of new insurance solutions such as cyber BI policies or non-damage BI coverage, which indemnifies a business for lost revenue due to disruption from an event. AGCS also utilizes semantics analysis to better understand supply chain risk. This enables mapping of supplier relationships down to the fourth tier in order to help identify any exposure or accumulation issues.

HOW MUCH CAN BUSINESS INTERRUPTION COST?



Average value of BI claim by cause of loss (selected).
Source: Allianz Global Corporate & Specialty

1 Business interruption and cyber incidents are tied at the top of the ranking at 37%. However business interruption received more responses by number – 1,078 to 1,052

2 Based on analysis of 1,175 corporate insurance claims which have both a property damage and business interruption loss component

3 BBC News, Yellow vest protests 'economic catastrophe' for France, December 9, 2018

4 The Guardian, UK running out of food warehouse space as no deal Brexit fears rise, November 18, 2018

(=) 2019: 2 (37%)

2 MAJOR RISKS IN FOCUS
CYBER INCIDENTS

Cyber risk takes center stage, as businesses struggle with major system outages, large data breaches and an emerging conflict threat.

5-year risk ranking (% of responses and position):
2018 2 (40%)
2017 3 (30%)
2016 3 (28%)
2015 5 (17%)

Top risk in:
- Austria
- Belgium
- Brazil
- France
- Hong Kong
- India
- New Zealand
- UK

Top risk in the following sectors:
- Aviation
- Entertainment & Media
- Financial Services
- Government & Public Services
- Professional Services
- Technology
- Telecommunciations

For the first time, **cyber incidents** is neck-and-neck with **business interruption (BI)** at the top of the Allianz Risk Barometer – with the two risks increasingly interlinked, reflecting the magnitude of the threat now posed by a growing dependence on technology and the malicious actions of nation states and criminals.

Incidents, such as cyber crime, privacy breaches, BI (including ransomware and distributed denial of service (DDoS) attacks) can trigger extensive losses. Cyber crime generates the headlines but often it is more mundane technical failures, IT glitches or human error which frequently cause system outages or data losses for business. The fall-out can be costly. According to AGCS analysis of insurance industry claims over the past five years, even the average insured loss from a cyber incident is now in excess of €2mn ($2.3mn) compared with almost €1.5mn from the average claim for a fire/explosion incident[1], with losses from the largest events in the hundreds of millions or higher.

Increasing concern about cyber incidents follows a watershed year. In the wake of the highly disruptive global WannaCry and NotPetya malware attacks, 2018 witnessed a stream of major IT outages, mega data breaches and privacy scandals, as well as landmark data protection rules in the EU's General Data Protection Regulation (GDPR).

"Cyber risk has been a major risk for a number of years, ever since IT moved from being a support function to a core, business-critical asset," says **Marek Stanislawski, Deputy Global Head of Cyber and Tech PI, AGCS**. *"Finally we have reached an important point where cyber is equally concerning for our customers as their major 'traditional' exposures, which means that entities across all industries and business segments now have this risk firmly on their radars."*

MEGA DATA BREACHES AND ATTACKS SOAR

As organizations hold more and more personal data, breaches are increasing in size and cost.

Recent mega data breaches include Equifax (143 million individuals), Facebook (50 million) and Uber (57 million). Meanwhile, the data breach which impacted around 380 million[2] customers of Marriott hotels at the end of 2018 is one of the largest on record.

The number of cyber-attacks worldwide doubled in 2017 to 160,000, although endemic underreporting means the true figure could be as high as 350,000, according to the Online Trust Alliance[3]. At the same time, the average cost of a cyber-attack has increased 62% over the past five years, according to Ponemon Institute and Accenture[4]. A typical data breach now costs a company $4mn, according to Ponemon, but very large breaches can cost hundreds of millions – the cost of the Marriott breach is estimated between $200mn and $600mn by AIR Worldwide[5].

RISING REGULATION AND LITIGATION

An important factor driving the cost of data breaches is regulation and litigation. In May 2018, the GDPR entered force, introducing greater privacy rights for consumers and greater enforcement powers for regulators, backed by the threat of large fines. Other jurisdictions have since announced plans to introduce tougher privacy laws inspired by the GDPR ranging from California to Brazil to India. Canada and Australia have also established mandatory breach notification regimes, in line with the GDPR and similar requirements in the US.

"GDPR and similar regulations are the 'new normal' in which we all need to find our way to operate," says Stanislawski.

Cyber incidents are also increasingly likely to spark litigation, including securities and consumer class actions. Data breaches, IT outages and cyber security incidents can generate large third party liabilities, as data subjects, shareholders and supply chain partners seek to recoup losses from companies and in some cases their directors.

Already a feature of US data breaches, class actions have spread to Europe, giving consumers the right to claim non-financial damages, such as for distress. A number of recent data breaches, including that of British Airways, one of the first significant breaches under the GDPR, have triggered class actions in the UK while a landmark case against Morrisons has seen the retailer held vicariously liable for a breach in the UK's first successful data breach class action[6].

EVOLVING THREATS

Cyber crime has become pervasive as criminals use more innovative methods to steal data, commit fraud or extort money. Worldwide, cybercrime costs an estimated $600bn a year[7], according to the Center for Strategic and International Studies (CSIS), up from $445bn in 2014. This compares with a 10-year average economic loss from natural catastrophes of around $208bn[8] – three times as much.

However, the past year has also witnessed a growing threat from nation states, which increasingly use technology to play out rivalries and conflicts, with implications for businesses. Nation states and affiliated hacker groups have targeted universities and public sector agencies, looking to steal valuable data and trade secrets, as well as the networks and industrial control systems (ICS) of critical infrastructure companies. NotPetya was attributed to Russian-backed hackers targeting Ukraine while energy companies in the Middle East have been hit with destructive malware attacks.

IOT AND NEW TECH

Advancements in technology are also generating new cyber threats and vulnerabilities. Organizations are concerned about the effect of increasing interconnectivity and developments such as automation and artificial intelligence.

Vulnerability is also growing with the increase in connected devices, with the Internet of Things (IoT), Industry 4.0 and digitalization of supply chains, which create new attack fronts for criminals and nation states to exploit.

According to cyber security firm Kaspersky, over three quarters of the companies it surveyed expect to become a target of a cyber security attack in the ICS space[9]. However, only 23% are compliant with minimal cybersecurity guidance or regulations of ICS. In 2016, a DDoS attack against internet company Dyn used a botnet army of corrupted IoT devices, while December 2018 saw hackers take control of 50,000 connected printers around the world to create posters supporting vlogger PewDiePie[10].

"SILENT CYBER" BECOMES MORE NOISY

The WannaCry and NotPetya malware attacks highlight the growing risk of BI *(see page 14)* and even physical damage from malware and other cyber incidents. They also have accelerated discussions around cyber insurance and in particular the need for affirmative cover.

The NotPetya attack is expected to generate around $3bn in losses for insurers, according to Property Claims Services. However, some 90% of this total can be attributed to so-called "silent cyber" exposure, with only 10% covered by affirmative cover. Non-affirmative cover is where cover for cyber incidents may exist in traditional property/casualty (P&C) policies, even though this was not the intention of the underwriter.

"Silent" or non-affirmative cyber exposures lead to inadequate protection for businesses with a lack of certainty and transparency for all parties involved. As part of a group-wide project, Allianz has reviewed cyber risks in its P&C policies in the commercial, corporate and specialty insurance segments and developed a new underwriting strategy to address "silent cyber" exposures.

"We will make it clear how cyber risks are covered in traditional policies and for which scenarios a dedicated cyber insurance solution is needed," says **Emy Donavan, Global Head of Cyber and Tech PI, AGCS**.

"Risk transfer is a vital element of cyber risk management, but, today, cyber insurance goes beyond this," adds Stanislawski. "It can be a valuable part of incident response, providing companies with contacts to specialists and consultants who can help battle the incident but also better prepare for events before they happen.

"Every company needs to adopt an IT security position which is adequate to its size, operations and risk profile and invest in technological security solutions, proper backup mechanisms and staff training. The last aspect is possibly the easiest one to miss but is equally important, especially for small- and mid-sized enterprises.

"Companies need to think about all of their employees as members of the cyber security team and provide them with proper training and empowerment to transform their staff from the 'weakest link' to the 'first line of defense'."

1 Allianz Global Corporate & Specialty, Average cyber loss value based on 115 claims with cyber as cause of loss. Average fire/explosion loss value – Global Claims Review, The Top Causes of Corporate Insurance Losses

2 Reuters, Marriott cuts estimate on size of massive Starwood hack, January 4, 2019

3 Online Trust Alliance, Cyber Incidents Trends Report, January 2018

4 Accenture, 2017 Cost of Cyber Crime Study

5 AIR Worldwide, AIR estimates losses for the Marriott breach will be between USD 200 million and USD 600 million

6 BBC News, Morrisons loses data leak challenge, October 22, 2018

7 Center for Strategic and International Studies, Economic Impact of Cybercrime – No Slowing Down

8 Swiss Re, Preliminary sigma estimates for 2018, December 18, 2018

9 Kaspersky, The State of Industrial Cybersecurity 2018

10 BBC News, PewDiePie printer hackers strike again, December 16, 2018

SPOTLIGHT ON...

CYBER BUSINESS INTERRUPTION

Whether resulting from cyber-attacks or, more frequently, from system outages or failures, cyber incidents are now a major cause of business interruption for today's networked companies whose primary assets are often data, service platforms or their groups of customers or suppliers.

Business interruption (BI) following a cyber incident has emerged as a key risk for businesses, with an increasing number of scenarios leading to disruption. For the first time in the Allianz Risk Barometer, survey participants indicated that cyber incidents were of a similar level of concern to the closely related risk of BI, which has ranked as the top peril in the survey over the past seven years.

For many companies, this is where their big exposure lies today. Think of a large organization that has a very sophisticated supply chain and an operation that produces millions of dollars in revenue – daily or monthly. Depending on the size of the organization, if it shuts down for technical issues in a cyber incident, that will trigger a significant loss.

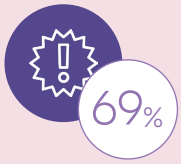
"As all businesses embrace digital business models, success is highly dependent on the technology facilitating the business," says **Georgi Pachov, Global Practice Leader, Cyber, AGCS**. *"Revenue streams can be easily interrupted following abnormal technological behavior. Cyber incidents leading to BI will become much more frequent in future due to the massive reliance on technology and data for running businesses. In the age of the 'Internet of Things', if two manufacturing devices cannot communicate and exchange data with each other this will inevitably lead to a business disruption."*

LOSS ACTIVITY

Business interruption was a hallmark of the WannaCry and NotPetya malware attacks in

WHAT ARE THE MAIN CAUSES OF ECONOMIC LOSS AFTER A CYBER INCIDENT?

Source: Allianz Global Corporate & Specialty. Figures represent the percentage of answers of all participants who responded (968). Figures don't add up to 100% as up to three risks could be selected.



1. Business interruption, impact on digital supply chains (loss of revenue)

2. Loss of reputation

3. Liability claims after a data breach (e.g. from other businesses, people)

4. Reinstatement/ data restoration costs

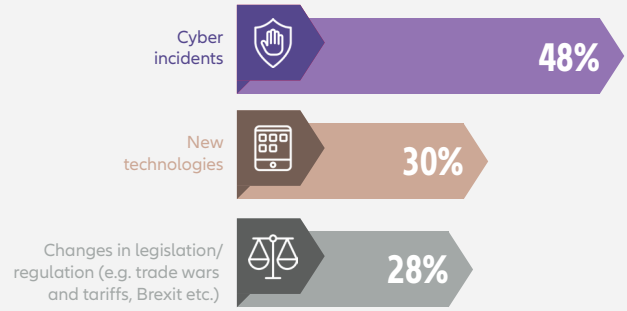
5. Fines and penalties

"The variety of cyber incidents occurring on a daily basis and hitting the headlines, coupled with the 'digital strategy' on every board's agenda, makes it clear: staying relevant and competitive requires innovation and technological advances while also becoming more exposed to cyber threats," says **Georgi Pachov, Global Practice Leader, Cyber, AGCS**. *"Finding the right balance between embracing innovation for business growth and managing the digital risks associated with that is crucial. Cyber BI insurance can be a key component in enabling this."*

2017, causing large losses for a number of shipping, logistics and manufacturing companies. Companies such as Maersk and FedEx saw losses of $300mn from the NotPetya event, while consumer goods manufacturer Reckitt Benckiser reported £100mn ($130mn) in loss revenues.

Malware attacks have continued to trouble companies – semiconductor maker Taiwan Semiconductor Manufacturing Company, a key supplier to Apple, lost over a day of production after a virus infected machinery at plants in Taiwan in August, 2018. The virus was a variant of WannaCry. Meanwhile, the ports of Barcelona and San Diego were both victims to ransomware attacks which impacted servers and administrative systems in September 2018, as was the shipping company COSCO in July, which also saw its IT systems disabled in the US. Insurers have seen a growing number of BI claims trigged by cyber incidents with claims that exceed $100mn[1].

WHAT ARE THE TOP EMERGING BUSINESS RISKS FOR THE NEXT THREE TO FIVE YEARS?



Source: Allianz Global Corporate & Specialty.
Figures represent the percentage of answers of all participants who responded (2,415). Figures don't add up to 100% as up to three risks could be selected.

FREQUENT HUMAN ERROR AND TECHNICAL FAILURE

Cyber incidents rank as the BI trigger most feared by businesses, and BI is also the biggest cause of economic loss for businesses after a cyber incident, according to Allianz Risk Barometer respondents. Loss of revenues and additional costs of working can be incurred from malicious acts, but more often than not are the result of technical glitches or human error. According to the Financial Conduct Authority (FCA), only 18% of all cyber incidents reported to the UK regulator were cyber-attacks[2], while 82% were the result of technology issues. Meanwhile, analysis of data breaches by Kroll found that 88% of data breaches were caused by human error, and just 12% were the result of a cyber-attack[3].

GROWING OUTAGE AND CBI EXPOSURES

IT outages have emerged as a significant exposure as organizations become reliant on technology to conduct everyday business. The airline sector has experienced a number of technology-related outages, including a major outage in 2017 which occurred after a power surge on reconnection knocked out British Airways systems over a holiday weekend affecting 75,000 passengers and costing it £80mn, according to initial estimates[4].

Customers at UK bank TSB suffered months of disruption in 2018 after a failed IT platform migration – the incident cost the bank in excess of €300mn[5]. The FCA says bank outages have risen 138% in the past year[6].

Reliance on IT and technology service providers – such as cloud services, online booking platforms and supply chain systems – also brings potential contingent business interruption (CBI) exposures. A software glitch at network equipment provider Ericsson disrupted services for millions of mobile phone customers in Europe and Japan in 2018[7]. When Visa suffered an outage in 2018, it affected the payment card services used by banks and retailers across Europe. Similarly, in 2017, a four hour outage at Amazon's AWS cloud computing division impacted a number of internet services, websites and other businesses. It was reported the outage was caused by human error. Guidewire Cyence Risk Analytics estimated that companies in the S&P 500 dependant on Amazon's services lost approximately $150mn as a result[8].

It has been estimated that in the event of an outage at a cloud service provider lasting more than 12 hours losses could total as much as $850mn in North America and $700mn in Europe, based on 50,000 companies in three specific industry sectors (financial, healthcare and retail) being impacted by the outage in each region[9].

"A single point of failure can trigger a chain reaction across the value chain, including suppliers to the final customer, and cause a severe business interruption and accumulation for insurers," says Pachov. *"The same event can trigger a significant reputational loss."*

1 Allianz Global Corporate & Specialty, Global Claims Review, The Top Causes of Corporate Insurance Losses
2 The Financial Conduct Authority, Cyber and technology resilience in UK financial services, November 27, 2018
3 Kroll, Data breach reports to Information Commissioner increase by 75%, September 4, 2018
4 Financial Times, BA faces £80m cost for IT failure that stranded 75,000 passengers, June 15, 2017
5 Reuters, Spain's Sabadell exceeds forecasts despite TSB outage costs, October 26, 2018
6 The Financial Conduct Authority, Cyber and technology resilience in UK financial services, November 27, 2018
7 Reuters, Ericsson sorry for software glitch that hits mobile services in Britain and Japan, December 6, 2018
8 Guidewire Cyence Risk Analytics, MMC Cyber Handbook 2018, Evolution of Cyber Risks Quantifying Systemic Exposures
9 Guidewire Cyence Risk Analytics, Allianz Global Corporate & Specialty, Allianz Risk Barometer 2018

(=) 2019: 3 (28%)

3 MAJOR RISKS IN FOCUS
NATURAL CATASTROPHES

As economic losses caused by disasters increase and concern over climate change grows, both businesses and their insurers need to stay on top of changing exposures around the world in order to effectively manage natural catastrophe risk.

5-year risk ranking (% of responses and position):
2018: 3 (30%)
2017: 4 (24%)
2016: 4 (24%)
2015: 2 (30%)

Top risk in:
- Argentina
- Chile
- Indonesia
- Japan
- Turkey

Top risk in the following sectors:
- Engineering, Construction & Real Estate
- Marine & Shipping

More than 11,000 people either died or were reported missing as a result of catastrophe events in 2018 with an earthquake causing a tsunami in Sulawesi, Indonesia, in September 2018, resulting in the highest human toll of the year – over 3,500 estimated dead or missing. 2018 also brought approximately $146bn of economic losses from **natural catastrophes (e.g. storm, flood, earthquake)**, according to preliminary estimates from Swiss Re[1].

The reinsurer also estimated that insured losses alone from natural catastrophes and man-made disasters in 2018 will reach $79bn, making it the fourth highest year ever, based on its **Sigma** research records. While higher than the annual average of the previous decade ($71bn), this total is down by half compared to 2017 ($150bn), which remains the costliest year on record for insurers, driven by the significant damage caused by three category 4+ hurricanes Harvey, Irma and Maria (HIM).

"Although there has not been a single major natural catastrophe event comparable in size with the 2017 hurricane events, the 2018 aggregated losses from multiple smaller and mid-sized events have led to considerable overall insured losses," says **Cosmin Tanasescu, Head of Catastrophe Risk Research & Development, AGCS**. *"We can think of 2018 as the 'little brother year of 2017' when it comes to the hurricane impact in the Northern Atlantic."*

Natural catastrophe activity is expected to account for over $70bn of 2018's insured catastrophe losses, with events such as hurricanes Michael and Florence in North America; typhoons Jebi and Mangkhut in Asia; wildfires in California; floods in India; and earthquakes in Japan, Indonesia and Papua New Guinea, contributing to this total loss figure. Although there may not have been an event of the magnitude of any of the HIM losses in the 2018 catastrophe year, significant activity was still evident. For example, 2018 is the second year of insurance payouts for wildfires exceeding $10bn in California alone following last year's Carr and Tubbs fires wreaking havoc on the state in 2017. Meanwhile, Typhoon Jebi became the most expensive typhoon on record, according to the General Insurance Association of Japan (GIAJ). It said it caused estimated insured losses of 585.1bn yen ($5.2bn) when it lashed the west coast of Japan in September 2018, resulting in widespread flooding and wind damage across the region. Reinsurer Munich Re has since estimated insured losses to be in the range of $9bn[2].

"Augmenting exposure and property values, as well as their concentration in high-hazard areas, have been the key drivers of the increase in natural catastrophe losses in recent decades," says **Carina Pfeuffer, Cat Risk Analyst, AGCS**.

NAT CAT ACTIVITY SEES RISE IN CLIMATE CHANGE RISK PERCEPTION

Allianz Risk Barometer respondents fear that recent natural catastrophe and extreme weather activity could be a harbinger of increasing financial losses and disruption ensuring **climate change/increasing volatility of weather** (8th, 13% of responses) rises to its highest-ever position in the global risk ranking *(see page 20)*.

Climate change is omnipresent in all regions around the world. Melting sea ice and polar ice shields resulting in rising sea levels, increasing permafrost thawing, droughts and heat waves in some areas and heavy precipitation in others are some of the commonly understood impacts of a warming climate. Generally, these impacts are expected to intensify in the coming decades.

Humans are adding enormous amounts of greenhouse gases to those naturally occurring in the atmosphere by burning fossil fuels, cutting down rainforests and farming livestock, which fuel the greenhouse effect and thus global warming.

"Overall economic losses caused by natural disasters are increasing worldwide," says Tanasescu. *"Both insureds and insurers need to stay on top of changing exposures around the world in order to effectively manage natural catastrophe risk."*

Extreme events are expected to change in intensity and frequency: increased wind speeds in tropical storms are projected as well as intensified heat waves and droughts for the US. For example, by 2050 the wildfire season in the western US is expected to be about three weeks longer. Therefore more burned areas are to be expected in future. For Atlantic and Eastern North Pacific hurricanes, increased precipitation rates and intensities are projected. Europe faces more frequent flash and pluvial floods. In Asia, more rain is projected on overall fewer rainy days, leading to more flooding but less rainwater that gets the chance to actually percolate underground to recharge aquifers.

"The consequences of climate change are diverse and heterogeneous by geography and are on the rise," says Tanasescu. *"The impact assessment of climate change on natural catastrophe events is an active area of research and requires detailed differentiation by peril and geographic region."*

FLOOD VERSUS WIND

Hurricanes Florence and Harvey in 2018 and 2017 respectively have shown the multi-dimensional risk aspects of severe storm activity. With both of these events, the flooding component was more concerning than the losses caused by wind, which emphasizes the need to manage natural catastrophe risk in a more holistic way to truly effectively assess and mitigate the impact from hurricanes.

In future, further improvements to the modeling and forecasting of extreme weather events remains key, says Tanasescu. Hurricane Florence was initially forecast to make landfall as a major hurricane but was then downgraded to a Category 1 event just before it hit Wrightsville Beach, North Carolina, in September 2018. Total precipitation amounts causing landslides and flash floods were highly unpredictable while the track forecast was actually fairly accurate.

HOW COMPANIES CAN PROTECT THEMSELVES

In order to help businesses mitigate their exposures and reduce the impact of natural catastrophe activity, insurers such as AGCS are using a range of sophisticated catastrophe management tools to monitor storms and assess natural catastrophe activity. AGCS' **Client Risk Profile** service highlights the key perils for a business' locations by using detailed hazard and advanced modeling information. According to Tanasescu, as a result, businesses can gain a better understanding of their catastrophe risks, ascertain their risk management strategies and identify appropriate mitigation measures, including optimization of their insurance coverage according to their own risk appetite.

"A key element of disaster preparedness is emergency scenario planning which involves among many other aspects, the analysis of the supply chain," says Tanasescu. *"This is why AGCS is evaluating various approaches and methodologies to to continuously improve our supply chain risk management capabilities. In the planning of future sites, companies should take into account the specific natural hazard risk profile and also think ahead by assessing future risk levels due to direct or indirect impacts of climate change."*

↘ **For a detailed overview of windstorm preparedness checklist**

↘ **For what to do before, during and after a flood to minimize potential damage checklist**

↘ **For a detailed overview of earthquake preparedness checklist**

1 Swiss Re, Preliminary sigma estimates for 2018, December 18, 2018

2 Munich Re, The natural disasters of 2018 in figures, January 8, 2019

TOP BUSINESS RISKS: 4-10

4

CHANGES IN LEGISLATION AND REGULATION

27% ▲ 2018: 5 (21%)

2018 was a turning point for global trade, according to **Ludovic Subran, Chief Economist of Euler Hermes and Deputy Chief Economist of Allianz**. US tariffs went up to 5.2% from 3.5%, bringing them back to the mid-80s and breaking with a history of preferring more sophisticated protectionism, such as regulation, over tariffs. Yet, the end-of-year trade truce with China is only postponing growing US-China rivalry as the backdrop for multinationals in 2019. As multilateral institutions struggle for a second wind, the rules of the games will be different for companies according to their shareholders, their location or the market they are after.

Some countries have beefed up anti-acquisition legislations (USA, France and Germany), others fear further sanctions (Russia, Iran and Cuba). Supply chains are at risk, and trade diversion starts to be a conversation in the boardroom to avoid negative effects of the new trade regime. In the meantime, in Europe, for example, member states have signed new free-trade agreements (the EU with Canada and Japan) and tried to reinforce their core. In 2019, risks loom for Europe with tense elections, fewer growth prospects for the Euro-zone and **Brexit fatigue**. What looks like a soft landing could become a forced landing if negative political outcomes and surprising regulatory moves spook investors and companies.

5

MARKET DEVELOPMENTS

23% ▼ 2018: 4 (22%)

2018 was marked by record volatility, divergence and surprises. 2019 should be under the same auspices, says **Ludovic Subran, Chief Economist of Euler Hermes and Deputy Chief Economist of Allianz**. Last year high US growth entailed tighter financing conditions especially in emerging markets. Oil prices also ranged between $57/bbl and $87/bbl, creating negative surprises for oil importers over the fall.

Divergence between the US and the rest of the world was very visible with higher growth in the US contrasting with the slowdown in Europe and Asia. Financial markets also went through rough rides as surprises on data breaches and negative news on zombie companies (highly indebted compared to their profits) corrected stock prices. In addition, multinationals, especially exporters, were negatively perceived in the context of trade wars. For example, automotive companies have been through a perfect storm: mobility disruption, trade war, and regulatory shocks. Through 2019, the cost of uncertainty will prevail, as well as rapidly changing political backdrops and possibly the return of risk of expropriation and confiscation. Market consolidation continues in vulnerable sectors (energy, machinery and equipment, retail).

FIRE, EXPLOSION

19% (=) 2018: 6 (20%)

Insurance industry loss research by AGCS shows that fire and explosion incidents cause the largest claims for insurers and the businesses they cover. Such events account for almost a quarter (24%) of the value of more than 470,000 corporate insurance industry claims analyzed over a five-year period up to 2018, compared with the second major cause of loss which is aviation collision/crash (14%)[1].

This means that fire and explosion incidents such as building/factory fires, electrical fires and gas explosions (but not including wildfires) have caused in excess of €14bn ($15.9bn) worth of insurance losses from more than 9,500 claims and are responsible for more than half (11) of the 20 largest non-natural catastrophe loss events analyzed over the past five years. As industries such as manufacturing have become more efficient, values at risk per square meter have risen exponentially meaning claims and losses are much more expensive than a decade ago. Even the average claim from a fire/explosion incident totals almost €1.5mn at €1.47mn today.

NEW TECHNOLOGIES

19% (=) 2018: 7 (15%)

New technologies present fantastic opportunities for business, including new ways to manage and reduce risk. However, new technologies also bring risk, sometimes with unexpected consequences. For example, illegal drone activity led to the cancellation of some 1,000 aircraft at Gatwick airport in the UK in December 2018.

By 2025, the "Internet of Things" is expected to comprise more than 100 billion connected devices with sensors collecting data from homes, factories and supply chains. *"This means better risk assessment through predictive indicators and more flexible, tailored and timely solutions,"* says **Michael Bruch, Global Head of Liability Risk Consulting/ESG, AGCS**. At the same time, connected devices raise questions around cyber security, data protection, business continuity and liability, and increase the potential for critical infrastructure breakdown.

"There is the opportunity to create greater transparency in the security and reliability of new technologies," says Bruch. *"The insurance industry, with new innovative partners, can drive the development of risk-based services. In an increasingly networked world, the aim must be to understand and manage risks more quickly and prevent losses before they occur."*

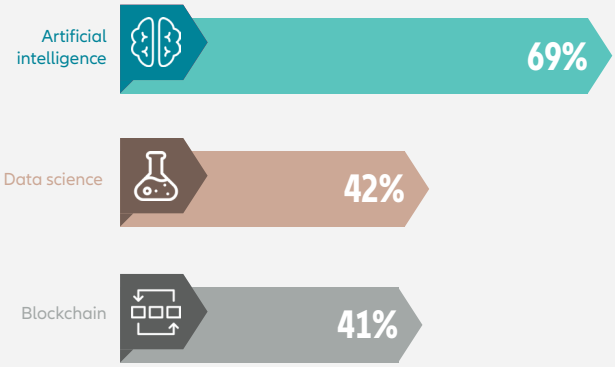
AGCS already partners with a number of insurtechs on initiatives such as utilizing machine learning to identify next generation litigation risks.

1 Allianz Global Corporate & Specialty, Global Claims Review, The Top Causes of Corporate Insurance Losses

NEW TECHNOLOGIES

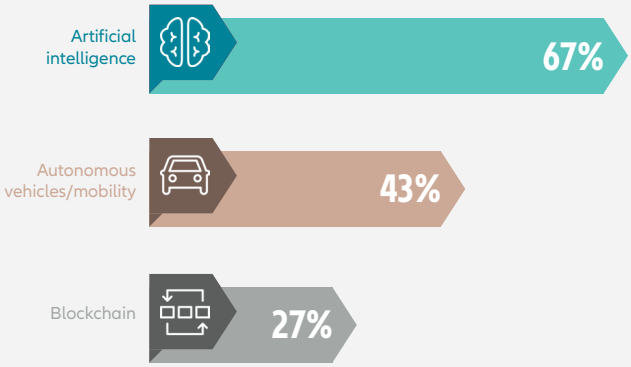
Digital ecosystems and platforms will provide the basis for a range of risk mitigation services that prevent damage before it occurs. At the same time, concerns about the use, accuracy and security of data are increasing.

WHICH NEW TECHNOLOGIES ARE THE MOST USEFUL OR VALUABLE?



Source: Allianz Global Corporate & Specialty.
Figures represent the percentage of answers of all participants who responded (505).
Figures don't add up to 100% as up to three risks could be selected.

WHICH NEW TECHNOLOGIES COME WITH THE GREATEST RISK POTENTIAL?



Source: Allianz Global Corporate & Specialty.
Figures represent the percentage of answers of all participants who responded (505).
Figures don't add up to 100% as up to three risks could be selected.

CLIMATE CHANGE/INCREASING VOLATILITY OF WEATHER

13% ▲ 2018: 10 (10%)

Hurricanes, tropical cyclones and wildfires broke records in 2017 and 2018 – insured losses from global catastrophes were $150bn in 2017, the highest ever. The US National Climate Assessment warned that inaction over climate change will lead to more intense storms, floods, droughts, heatwaves and wildfires, generating hundreds of billions of dollars in annual losses by the end of the century. The rising cost of climate change is already noticeable. Analysis shows the number of weather-related/flood loss events has increased by a factor of three to four since 1980[2].

Left unchecked, climate change is likely to have huge economic, political and social impacts – with implications for food and water security, health, migration and conflicts. Indirect consequences include cultural and behavioral change (for example, the sudden shift in consumer opinion around plastics or investors' views on fossil fuels). Climate change will also have big implications for regulation and liability. Emissions regulations and targets are already shaping industries like aviation and shipping, while growing climate change reporting and disclosure requirements will increase exposures for directors and officers.

2 Munich Re, Trends in weather-related disasters - consequences for insurers and society, March 2016

LOSS OF REPUTATION OR BRAND VALUE

13% ▼ 2018: 8 (13%)

A company's reputation is its most valuable asset. Product recalls, cyber incidents, industrial disputes and executive conduct have all tainted the reputations of organizations in recent years, affecting the likes of airlines, car manufacturers and banks. The value of Facebook fell almost 40% in 2018 after a turbulent year which included it being embroiled in a privacy scandal and a massive data breach[3].

Protecting reputation and brand has taken on urgency in the social media age. There are an estimated three billion social media users worldwide, while Facebook Messenger and WhatsApp handle 60 billion messages a day ensuring a reputational incident can quickly escalate out of control, but social media can also help companies monitor and engage with customers. A study of 125 reputational events over the past decade by Pentland Analytics and Aon[4] found the impact of reputation events on stock prices has doubled since the introduction of social media. Effective planning and crisis management has become essential. It is estimated a company could add as much as 20% of value or lose up to 30% depending on its reputation risk preparedness and management in the immediate aftermath of a crisis. Insurance can also provide tangible assistance to an intangible risk, such as funding advisory and crisis response costs.

SHORTAGE OF SKILLED WORKFORCE

9% ▲ 2018: 15 (6%)

Shortage of skilled workforce appears in the top 10 global risks for the first time with many factors such as changing demographics, a shallow pool of talent in the digital economy and Brexit uncertainty contributing to its rise.

"Skilled workforce — and human capital more generally — has become the scarce resource of the digital economy," says **Ludovic Subran, Chief Economist of Euler Hermes and Deputy Chief Economist of Allianz**. *"Competition is fierce to get new recruits with competencies in artificial intelligence, data science, or 'frontier risk management' such as managing cyber or reputational risk as most of these jobs did not exist 10 years ago. Even attractive salaries do not suffice as the pool of recruits with the needed skillset is limited and the urgency to onboard them does not allow for on-the-job training."*

Regulatory change can also negatively impact. A UK study[5] found that nine in 10 employers were struggling to recruit the skilled staff they need, with Brexit set to make this worse. New talent must be recruited quickly. *"Managers must embrace the technological acuity of younger employees,"* says **Scott Steinmetz, Global Head of MidCorp Risk Consulting, AGCS**. *"They must also focus on disruptive technologies and ideas, as these may bring beneficial innovations. Machine learning and automation can offset worker attrition, but requires significant investment."*

3 CNBC, Here are the scandals and other incidents that have sent Facebook's share price tanking in 2018, November 20, 2018
4 Pentland Analytics and Aon, Reputation Risk In The Cyber Age - The Impact On Shareholder Value, August 2018
5 The Independent, Nine in 10 UK employers struggling to find skilled workers with Brexit set to make shortage worse, survey finds, June 12, 2018

SME BUSINESS RISKS

Awareness of the growing cyber threat and its link to loss of reputation, weather woes and the impact of changes in trade agreements, are the major worries for multinational SME businesses.

Taken together, total responses from small- to mid-sized (SME) business experts account for about half of the total Allianz Risk Barometer responses (1,437 of 2,882). Business interruption (BI) is the top risk for mid-sized enterprises (annual revenues over €250mn but under €500mn) replacing cyber incidents in the top spot year-on-year. Coincidentally, cyber incidents is the top risk for small-sized enterprises (annual revenues under €250mn), replacing BI which was the top risk in 2018.

CYBER AWARENESS GROWING

SME companies increasingly recognize their cyber exposure and are more apt to secure adequate insurance cover than in the past, says **Rajiv Iyer, Global Head of MidCorp Package, Small Business and Casualty, AGCS**.

"This stems from the fact that advances in cloud computing and social media have increased small companies' exposures while large data breach events, such as the Equifax breach and numerous other cyber security-related issues have necessitated greater protection of customer data. SME businesses see the need for adequate cyber cover to feel more protected in case of an event such as a breach."

BI EXPOSURES STILL RELEVANT

While cyber incidents increased in the small-sized company space, BI drops from first place to fifth in the ranking for 2019. For mid-sized companies, however BI is the top risk concern. Iyer believes that BI claims, while admittedly lower in value for SME businesses, remain an issue. A severe interruption can even have a terminal impact for smaller-sized companies, given the effect it can have on income and revenues. Iyer sees significant BI exposure among SME businesses from natural catastrophe activity, cyber risk and changes in legislation *(see page 23)*.

WEATHER WOES

Natural catastrophe and weather volatility is another major concern for SME businesses. Natural catastrophes

Top 5 risks for small enterprise companies (<€250mn annual revenues)

Rank		Percent	2018 rank	Trend
1	**Cyber incidents (e.g. cyber crime, IT failure/outage, data breaches, fines and penalties)**	**32%**	2 (30%)	▲
2	Changes in legislation and regulation (e.g. trade wars and tariffs, economic sanctions, protectionism, Brexit, Euro-zone disintegration)	**30%**	5 (22%)	▲
3	Natural catastrophes (e.g. storm, flood, earthquake)	**27%**	3 (28%)	=
4	Market developments (e.g. volatility, intensified competition/new entrants, M&A, market stagnation, market fluctuation)	**27%**	4 (27%)	=
5	Business interruption (incl. supply chain disruption)	**26%**	1 (33%)	▼

Source: Allianz Global Corporate & Specialty. Figures represent how often a risk was selected as a percentage of all responses for that company size. Responses: 818. Figures don't add up to 100% as up to three risks could be selected.

Cyber incidents ranks as the top risk for small enterprises (32% of responses), up from 2nd (30%) year-on-year, and as the second most important peril for mid-sized companies.

"SMEs worry about cyber-attacks and data breaches because their internal organization may not be as strong as larger companies," says **Volker Muench, Global Practice Leader, Utilities & Services, IT Communication, AGCS**. *"Survey results have shown that many SMEs have had data security problems, but have not always reported them because they were afraid of the reputational damage this could cause, such as a loss of contracts. We see a clear relationship between cyber and loss of reputation, especially for SMEs."*

↘ View the full risk rankings for large, medium and small companies

↘ View the full risk rankings for 22 industry sectors

remains in third position year-on-year for both small- and mid-sized companies while climate change/increasing volatility of weather appears in both top 10 risk rankings.

"The recent significant increase in windstorm, wildfire and hurricane activity has created the need for adequate property and BI coverage for lost income," says Iyer.

Further, Iyer believes that the US decision to quit the Paris Climate Treaty, as well as to focus on coal and relax environmental regulations, may exacerbate the effects of global warming.

"'Unprecedented' is used to describe the last couple of years in terms of natural catastrophe events and, while this activity might be cyclical in nature, for now it is a reality with no abatement in sight," says Iyer.

TRADING IMPACTS

One risk concern that has increased significantly in both the small- and mid-enterprise space is changes in legislation – from fifth to second year-on-year for small-sized companies and from sixth to fourth for mid-sized firms. Renewed populism in many countries, as well as changes in trade agreements and outright trade wars, are affecting multinational SME businesses.

"Changes in the cost of goods based on tariff expansions and increased protectionism remain a volatile factor for our customers and businesses," says Iyer. *"This, in turn, causes swings in net income or cost of goods sold."*

SME OUTLOOK

In general, as the global economy slows down, SME businesses may see a residual slowdown in production in 2019. Tariff increases will have a residual effect on net income and operating cash flows for maintenance and upkeep of facilities. SME companies with diversified portfolios will be able to weather the possible downturn. Finally, cyber exposures will continue to threaten SMEs, while changes to governmental regulations on data security means SME insurers will have to tailor coverage to companies' exposure-based needs.

Top 5 risks for mid-size companies (€250mn to €500mn annual revenues)

Rank		Percent	2018 rank	Trend
1	**Business interruption (incl. supply chain disruption)**	**38%**	2 (37%)	▲
2	Cyber incidents (e.g. cyber crime, IT failure/outage, data breaches, fines and penalties)	**32%**	1 (39%)	▼
3	Natural catastrophes (e.g. storm, flood, earthquake)	**29%**	3 (32%)	=
4	Changes in legislation and regulation (e.g. trade wars and tariffs, economic sanctions, protectionism, Brexit, Euro-zone disintegration)	**24%**	6 (18%)	▲
5	Market developments (e.g. volatility, intensified competition/new entrants, M&A, market stagnation, market fluctuation)	**23%**	5 (21%)	=

Source: Allianz Global Corporate & Specialty. Figures represent how often a risk was selected as a percentage of all responses for that company size. Responses = 619. Figures don't add up to 100% as up to three risks could be selected.

Business interruption (BI) ranks as the top risk for mid-sized enterprises (38% of responses), up from 2nd (37%) year-on-year. The impact of changes in legislation and regulation is a rising risk concern for SMEs.

CONTACT US

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

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

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

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

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

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

UK
Michael Burns
michael.burns@allianz.com
+44 203 451 3549

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

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

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

For more information contact
agcs.communication@allianz.com

Follow Allianz Global Corporate & Specialty on

Twitter **@AGCS_Insurance #ARB2019** and

LinkedIn

www.agcs.allianz.com

Credits

Contributors:
Alejandra Larumbe Milla, Heidi Polke-Markmann, Patrik Vanheyden

Publications/Content Specialist:
Joel Whitehead (joel.whitehead@agcs.allianz.com)

Design:
Kapusniak Design

Images:
Adobe Stock/iStockPhoto

Editor:
Greg Dobie (greg.dobie@allianz.com)

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

January 2019