ALLIANZ RISK BAROMETER

TOP BUSINESS RISKS FOR 2018

The most important corporate perils for the year ahead and beyond, based on the insight of more than 1,900 risk management experts from 80 countries

Allianz

SNAPSHOT: TOP BUSINESS RISKS AROUND THE WORLD IN 2018

↘ View all country, regional and industry risk data here

Canada

1 (=) **Business interruption**
2 (▲) Cyber incidents
2 (▲) Natural catastrophes

"Business interruption (BI) can be a consequence of many of the other risks identified in the Risk Barometer. Whether it stems from a natural catastrophe or a cyber-attack, it is a daily concern for businesses."
ULRICH KADOW, CEO, AGCS CANADA

US

1 (▲) **Cyber incidents**
2 (▼) Business interruption
3 (=) Natural catastrophes

"Cyber is a 24/7 365-day-a-year risk that is evolving at a rapid pace. Cyber losses can span many risk areas, such as loss of reputation, BI and new technology. In addition, it is not limited to being an external risk exposure, as the actions of employees can impact a company's risk of data breaches or other forms of cyber incidents."
BILL SCALDAFERRI, AGCS BOARD MEMBER AND CEO, NORTH AMERICA

France

1 (=) **Business interruption**
2 (=) Cyber incidents
3 (▲) Fire, explosion

"In the Industry 4.0 era, as businesses rely more and more on digitalization to manage their supply chains, they face the new issue of cyber-driven BI."
CORINNE CIPIÈRE, CEO, AGCS FRANCE

Spain

1 (=) **Business interruption**
2 (▲) Natural catastrophes
3 (▲) Fire, explosion

"Spanish companies were especially impacted by the earthquakes, hurricanes and storms of 2017, ensuring natural catastrophes made a significant move in this year's Risk Barometer."
JUAN MANUEL NEGRO, CEO, AGCS SPAIN

UK

1 (=) **Cyber incidents**
2 (▲) Changes in legislation and regulation
3 (▼) Business interruption

"With an increase both in the demand for our cyber risk products and in volume of claims, it's no surprise to see cyber as the top risk again. Meanwhile, the challenging macro-economic environment, threat of terrorism, and uncertainty around Brexit will continue to drive up volatility. We need to adapt to the evolving landscape to help our clients understand, manage and protect against these complex risks in 2018."
BRIAN KIRWAN, CEO, AGCS UK

Italy

1 (=) **Business interruption**
2 (▲) Cyber incidents
3 (=) Natural catastrophes

"Underestimated for a long time, cyber risk is an increasing concern for Italian companies – moving up to second in the Risk Barometer, while loss of reputation is also a rising threat."
NICOLA MANCINO, CEO, AGCS ITALY

Germany

1 (▲) **Business interruption**
2 (▼) Cyber incidents
3 (▲) Natural catastrophes

"The new gold of the digital economy is intangible assets such as data, platforms, networks or the company's reputation. As a result of this shift, their protection is becoming more important in Germany. Business and supply chain disruptions, as well as cyber threats, are among the greatest risks today."
ANDREAS BERGER, AGCS BOARD MEMBER AND CEO, CENTRAL AND EASTERN EUROPE

Japan

1 (▲) **Business interruption**
2 (▲) Cyber incidents
3 (▲) New technologies

China

1 (▲) **Business interruption**
2 (▲) Cyber incidents
3 (▲) New technologies

Australia

1 (▲) **Cyber incidents**
2 (▼) Business interruption
3 (▲) Changes in legislation and regulation

"2017 was the costliest natural catastrophe year ever for insured losses. Despite most catastrophes occurring in North America and Mexico, they still impact Asia, as 50% of claims by value are from subsidiaries of multi-national companies located outside of the disaster zones. This reflects the need for companies to adopt a global approach to risk exposures and insurance coverage. As manufacturing shifts east, Asia is increasingly exposed to such disasters."
MARK MITCHELL, CEO AGCS ASIA

Nigeria

1 (▲) **Theft, fraud and corruption**
2 (=) Market developments
3 (=) Changes in legislation and regulation

South Africa

1 (=) **Cyber incidents**
2 (=) Business interruption
3 (▲) Changes in legislation and regulation

"Businesses in Africa are deeply concerned about the impact of business interruption, which is largely attributed to fire incidents, especially in developing markets. Political risks and violence; theft, fraud and corruption; and market developments are also a rising concern across the region. Cyber incidents feature prominently in South Africa and Morocco. This is not surprising as both countries are strong insurance markets."
THUSANG MAHLANGU, CEO, AGCS AFRICA

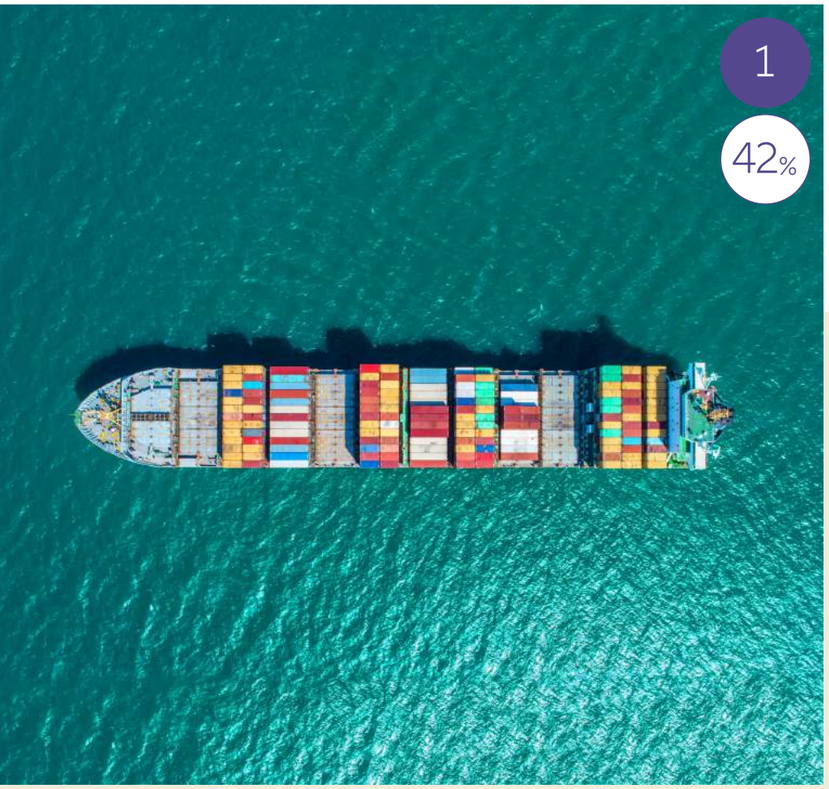
↘ View Africa & Middle East country risk data here

KEY

- (▲) **Risk higher than in 2017**
- (▼) **Risk lower than in 2017**
- (=) **No change in 2017**

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

CONTENTS



Source: Allianz Global Corporate & Specialty.
Figures represent the number of risks selected as a percentage of all survey responses (2,376). The 1,911 respondents could provide answers for up to two industries and up to three risks per industry.

ALLIANZ RISK BAROMETER

TOP 10 GLOBAL BUSINESS RISKS FOR 2018

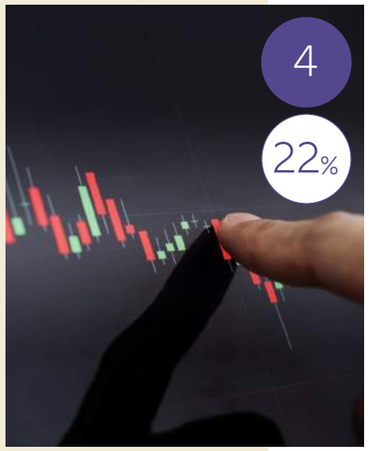
↘ View the full Risk Barometer 2018 rankings here

(=) 2017: 37% (1)

Business interruption
(incl. supply chain disruption)

(▲) 2017: 30% (3)

Cyber incidents
(e.g. cyber crime, IT failure, data breaches)



(▲) 2017: 24% (4)

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

(▼) 2017: 31% (2)

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

(=) 2017: 24% (5)

Changes in legislation and regulation
(e.g. government change, economic sanctions, protectionism, Brexit, Euro-zone disintegration)

(▲) 2017: 16% (7)

Fire, explosion

(▲) 2017: 12% (10)

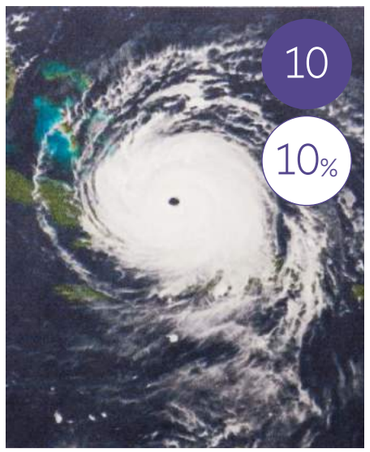
New technologies
(e.g. impact of increasing interconnectivity, nanotechnology, artificial intelligence, 3D printing, drones)

(▲) 2017: 13% (9)

Loss of reputation or brand value

(▼) 2017: 14% (8)

Political risks and violence
(e.g. war, terrorism, civil commotion)



(▲) NEW

Climate change/ increasing volatility of weather

KEY

- (▲) Risk higher than in 2017
- (▼) Risk lower than in 2017
- (=) No change in 2017
- (1) 2017 risk ranking

EXECUTIVE SUMMARY

Business interruption and cyber incidents interlink as the major threat for companies through 2018 and beyond, according to the insight of 1,911 risk experts from 80 countries in the Allianz Risk Barometer 2018.

Business interruption (BI) ranks as the most important global risk for the sixth year in a row (42% of responses), due to its tremendous effect on revenues. Companies face an increasing number of scenarios – from traditional exposures, such as the physical damage impact of natural catastrophes and fires on facilities and the supply chain to new triggers stemming from digitalization and interconnectedness that typically come without physical damage, but high financial loss. Cyber incidents is the most feared BI trigger for the first time. BI is also the main cause of economic loss for businesses after a cyber incident. Cyber BI incidents are increasing, resulting from hacker attacks, such as ransomware incidents, but more frequently from technical failures and employee error ↘ Page 8

Cyber incidents continues an upward trajectory to 2nd most important business risk (40%). Five years ago it ranked 15th. Like a natural disaster, an attack can potentially impact hundreds of companies and incidents have escalated. So-called "cyber hurricane" events, where hackers disrupt large numbers of companies through common internet infrastructure dependencies, are increasing. Meanwhile, the introduction of the General Data Protection Regulation (GDPR) across Europe in May 2018, brings the prospect of more, and larger, fines for businesses who don't comply. The way in which a business manages a data breach has a direct impact on the final cost. This will become even more the case under the GDPR. Reputational damage is irrevocably linked if the response to a cyber incident is inadequate. ↘ Page 10 Awareness of the cyber threat is soaring among small- to medium-sized businesses (SMEs) ↘ Page 16

A record-breaking $135bn in insured losses in 2017[1] ensures **natural catastrophes** returns to the top three business risks in 2018 (3rd 30%). Businesses worry the activity of the past year could be a harbinger of increasing intensity and frequency, ensuring **climate change** (10th 10%) is also a new entrant in the top 10 risks. Loss potential is further exacerbated by rapid urbanization in coastal areas. ↘ Page 12

Businesses are less concerned about **market developments** (4th 22%) than 12 months ago. Risk perception of **changes in legislation and regulation** (5th 21%) remains the same, despite a reduction in the number of protectionist measures. Concerns about **fire, explosion** (6th 20%) are up – claims analysis shows the average cost of a BI loss from a large fire incident totals $2m (€1.7m) – while **loss of reputation or brand value** (8th 13%) is also an increasing worry in an age when a crisis can spread globally within minutes. **Political risks and violence** (9th 11%) is down year-on-year, although businesses are more worried about the impact of terrorism. A general trend of increased political activism is anticipated in 2018. ↘ Page 14

The risk impact of **new technologies** (7th 15%) is one of the big movers in the rankings year-on-year. It is also the second top long-term risk after cyber incidents, with which it is closely interlinked. Vulnerability of machines to failure or malicious cyber acts will increase in future, potentially causing significant disruption to critical infrastructure. Businesses also have to prepare for new liability scenarios, as responsibility shifts from human to machine. ↘ Page 18

New risks require new tools to help manage and mitigate potential impacts. The role of insurance is evolving, whether it is through provision of new coverages such as cyber BI protection and non-damage BI which can protect against lost revenues due to an event disruption, or, increasingly, via offering access to services that can help to mitigate the impact of an incident as it develops, such as to crisis management specialists after a data breach or other reputational event. This reflects the fact that today's risk management world is more fluid than it has ever been, with the impact of many of the top **Allianz Risk Barometer** perils interlinked.

1 Munich Re NatCatService

ALLIANZ RISK BAROMETER METHODOLOGY

The seventh **Allianz Risk Barometer** is the biggest yet, incorporating the views of a record 1,911 respondents from 80 countries. The annual corporate risk survey was conducted among Allianz customers (global businesses) and brokers. It also surveyed risk consultants, underwriters, senior managers and claims experts in the corporate insurance segment of both Allianz Global Corporate & Specialty and other Allianz entities.

Respondents were questioned during October and November 2017. 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 most importance. As multiple answers for up to two industries were possible, 2,376 responses and 6,472 risk answers were recorded.

Most answers were for large enterprises (>€500m annual revenue) [1,257 responses, 53%]. Mid-sized enterprises (€250m to €500m revenue) contributed 516 responses (22%), while small enterprises (<€250m) produced 603 responses (25%). Risk experts from 22 industry sectors were featured.

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

All currencies US$ unless stated.

↘ Click here to view the full regional, country and industry risk data

1,911 respondents

80 countries

2,376 responses

22 industry sectors

(=) 2018: 42%/2017: 37% (1)

1 MAJOR RISKS IN FOCUS
BUSINESS INTERRUPTION

With more and more new loss triggers emerging, and an increase in cyber business interruption (BI) incidents, BI is the top risk in a "networked society"

5-year risk rankings (% of responses and position):
2017: 37% (1)
2016: 38% (1)
2015: 46% (1)
2014: 43% (1)

Top risk in:
- Canada
- China
- France
- Germany
- Hong Kong
- Indonesia
- Italy
- Japan
- Morocco
- Netherlands
- South Korea
- Spain
- Switzerland

Top risk in the following sectors:
- Aviation
- Food & Beverage
- Manufacturing (incl. Automotive)
- Power & Utilities
- Retailing & Wholesale
- Transportation

The threats may be changing but the result stays the same. **Business interruption (incl. supply chain disruption)** is the top risk for companies for the sixth consecutive year, according to the **Allianz Risk Barometer**, with 42% of responses rating it as one of the three most important risks companies face in 2018, up year-on-year. Whether it results from factory fires, destroyed shipping containers, or, increasingly, cyber incidents, BI can have a tremendous effect on a company's revenues. Yet its impact is one of the hardest risks to measure. A severe interruption can even have a terminal impact, particularly for smaller companies. Moreover, increasing interconnectivity means the potential for higher losses is growing. BI can be a consequence of many of the other top risks in this year's **Allianz Risk Barometer**.

AN INCREASING NUMBER OF DISRUPTIVE SCENARIOS

BI can be triggered by traditional property damages resulting from natural catastrophe losses or 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).

BI losses for businesses can often be much higher than the cost of any physical damage. The average large BI property insurance claim is now in excess of $2m[1]. This is more than a third higher than the average direct property damage loss. ($2.4m and $1.75m respectively).

But as many businesses transition from being rich in physical assets to deriving more value from intangibles and services, increasingly, BI is being triggered by non-traditional risk exposures which don't cause physical damage but result in lost income – so-called non-damage business interruption (NDBI).

"Businesses are facing an increasing number of disruptive scenarios, as the nature of BI risk evolves in our networked society," explains **Volker Muench, Global Practice Group Leader, Property, AGCS**. *"They still have to deal with traditional exposures, such as the impact of natural catastrophe activity, which we've seen peak in 2017. But they are also challenged by a multitude of new triggers stemming from digitalization – as data becomes a critical asset –, supplier interdependencies and product quality incidents, as well as the indirect impact from terrorism and political events or strikes, which can result in loss of income from people staying away from impacted areas."*

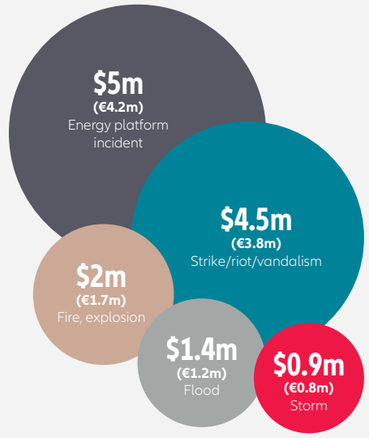
The threats don't stop there. In today's uncertain political and business landscape, where the prospect of an abrupt change of rules disrupting business models is an increasing concern, a withdrawal of regulatory approval or product license is another potential BI risk.

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

Source: Allianz Global Corporate & Specialty. Figures represent the percentage of answers of all participants who responded (845). Figures don't add up to 100% as up to three risks could be selected.

HOW MUCH CAN BI COST?



Average value of BI claim by cause of loss (selected). Energy platform and strike/riot/vandalism incidents are low frequency/high severity events.
Source: Allianz Global Corporate & Specialty

The rise of cyber BI and internet supply chain risk

For the first time in the **Allianz Risk Barometer** survey, the impact of cyber incidents (42% of responses) is ranked as the most feared BI trigger by businesses. BI also ranks as the main cause of an economic loss *(see page 11)* after a cyber incident (67% of responses). This represents a significant shift in the perception of BI risk from respondents over the past 12 months, reflecting the fact cyber incidents have escalated in scale. Events in 2017, such as the **WannaCry** and **Petya** ransomware attacks *(see page 10)*, have brought significant disruption and financial losses to a large number of businesses and services. Others, such as the massive distributed denial of service attack on internet provider Dyn in October 2016 *(see page 10)*, also demonstrate the interconnectedness of risks and shared reliance on common internet infrastructure, service providers and technologies, according to Cyence Risk Analytics, from Guidewire, which partners with AGCS in assessing cyber risk.

While cyber BI can result from the likes of ransomware incidents, which have doubled in frequency over the past year and involve hackers encrypting files and demanding compensation to unlock them, a more frequent cause of cyber BI can be mundane technical failures or employee error. For example, in February 2017, Amazon suffered an outage of its cloud storage service for four hours, impacting a number of internet services, websites and other businesses. It was reported the outage was caused by human error[2]. Cyence Risk Analytics estimates that companies in the S&P 500 dependant on Amazon's services lost approximately $150m as a result[3].

Cyence Risk Analytics notes that BI is one of the largest loss drivers for businesses after a cyber incident. For example, in the event of an outage at a cloud service provider lasting more than 12 hours, it estimates that losses could total $850m in North America and $700m in Europe, based on 50,000 companies in three specific industry sectors (financial, healthcare and retail) being impacted by the outage in each region.

RISK MITIGATION, SEMANTIC ANALYSIS AND AN INSURANCE EVOLUTION

In this year's Risk Barometer, BI also ranks as the second most underestimated risk *(see page 11)*.

"BI impact is easy to underestimate," says **Thomas Varney, Regional Manager Americas, Allianz Risk Consulting, AGCS**. *"Risks can be extremely complex. In many cases it is difficult to know what the actual exposure is, how to calculate the loss, or even where the actual disruption in the supply chain occurred."*

"Companies often underestimate the complexity of 'getting back to business' and can have bottlenecks in their emergency plans, particularly with regards to alternative suppliers," says Muench. *"Cyber risk is another example. They may have a cyber-attack continuity plan to start their own IT again but is the BI threat adequately assessed? What about the impact of a cyber incident at one of their suppliers stopping them from delivering products or services?"*

Nevertheless risks can be mitigated. *"Businesses should continuously fine tune their emergency plans to reflect the new BI environment, plan for a variety of scenarios and have strategic alignment through all departments on predictive detection of risks,"* says Muench.

Insurers such as AGCS can support businesses further through provision of new insurance solutions such as cyber BI and NDBI cover, which indemnifies a business for lost revenue due to disruption from an event. AGCS also leverages semantic analysis tools to better understand a business' supply chain risk. This enables mapping of supplier relationships up to the fourth tier, thus helping to identify exposure and accumulation issues.

"It's important that businesses understand that new NDBI triggers are evolving," says Varney. *"Today's threats may be understood, but what about tomorrow's? It's an ongoing diligence to keep abreast of the impacts that are going to change as a business evolves. Businesses need to understand the new facilities they have, mergers and acquisitions that may have occurred, different suppliers they may be using – all of these continually change as a business grows."*

1 Allianz Global Corporate & Specialty, Global Claims Review: Business Interruption in Focus
2 The Guardian, Typo blamed for Amazon's internet-crippling outage, March 3, 2017
3 Evolution of Cyber Risks: Quantifying Systemic Exposures, George Ng and Philip Rosace, Cyence Risk Analytics, Guidewire, MMC Cyber Handbook 2018

2018: 40%/2017: 30% (3)

2 MAJOR RISKS IN FOCUS
CYBER INCIDENTS

New threats such as "cyber hurricanes", increasing reputational risk and tougher data rules mean businesses and risk experts are more concerned than ever

5-year risk rankings (% of responses and position):
2017 30% (3)
2016 28% (3)
2015 17% (5)
2014 12% (8)

Top risk in:
- Australia
- Austria
- Belgium
- Brazil
- India
- Indonesia
- Netherlands
- Singapore
- South Africa
- UK
- USA

Top risk in the following sectors:
- Entertainment & Media
- Financial Services
- Professional Services
- Technology
- Telecommunications

Production of a vital vaccine is disrupted, leading to fears of a drug shortage. One of the world's busiest "smart" ports is brought to a standstill, leaving containers stranded. These and other recent events from the June 2017 **Petya** ransomware attack show how vulnerable businesses are to an ever-evolving cyber threat and its impact on the balance sheet – an estimated $275m[1] in insured losses alone from the vaccine incident and a potential $300m[2] hit for a shipping company from the terminal incident, and others. Economic losses from the **WannaCry** attack a month earlier could eventually hit $8bn, according to Cyence Risk Analytics. Just like a natural disaster, a single cyber-attack can potentially impact hundreds of companies, leading to severe business interruption and loss of customers and reputation. It is no wonder that cyber incidents continue a six year climb up the **Allianz Risk Barometer** in 2018 – cyber is now the top risk in 11 countries.

MULTIPLE THREATS UNDERESTIMATED

"Every company has been or will be impacted by cyber risk. It is not over-hyped. If anything it is under-appreciated because the threats are not always well understood," says **Emy Donavan, Global Head of Cyber at AGCS**, noting that over 50% of Risk Barometer responses rank cyber as the risk most underestimated by businesses. *"There are now multiple cyber threats to a company's digital presence."*

Personal data or intellectual property can be compromised. Businesses can incur network liability if a corrupted file is transferred to another company. Respondents are increasingly worried about new perils such as cyber extortion and, particularly, business interruption (BI) *(see page 9)*. Meanwhile, the emergence of two major security flaws in computer chips – Meltdown and Spectre – in January 2018, which raised fears that hackers could steal data from computers and devices around the world, shows how cyber interconnectivity continues to bring unexpected threats.

LARGER INFRASTRUCTURE ATTACKS IN 2018

Businesses worry about the increasing sophistication of cyber-attacks. December 2017 brought the first report of a successful safety system breach at an industrial plant by hackers, after previous incidents at other types of critical infrastructure[3]. Meanwhile, incidents such as WannaCry, Petya, and **Mirai**, the massive distributed denial of service (DDoS) attack on internet provider Dyn, which disrupted the likes of Twitter, CNN and Netflix in October 2016, are part of a growing trend of broader accumulation events, or "cyber hurricanes". Hackers can disrupt larger numbers of companies by targeting common internet infrastructure dependencies, for example – a trend that will likely continue through 2018.

"Companies of different sizes and industries need to pay attention to different threats to prevent core cyber risks such as BI," says Donavan. *"Small companies are likely to be crippled if hit with a ransomware attack, while larger firms are targets of a greater range of threats, such as the DDoS attacks, which can overwhelm systems. It is almost impossible to completely prevent cyber events but there are many approaches that can make the ones that happen far less damaging."*

One of the most effective prevention techniques for ransomware is effective, secure, segregated back-ups that are performed regularly, Donavan says. User-based access rights can also be effective. If the concern is a DDoS attack, systems redundancy and back-up servers are vital.

REPUTATION ON THE LINE

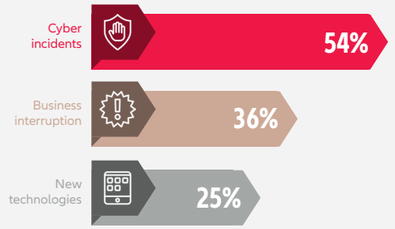
Cyber incidents aren't just caused by hackers. Technical failure or malicious or innocent employee action is often to blame. Whatever the cause, reputational damage is irrevocably linked. According to reputation analysis and research institute, MediaTenor, 75% of all companies which suffer a cyber-attack also incur reputational damage or loss[4]. Companies in the entertainment, banking and retail sectors are particularly vulnerable due to handling confidential data. Furthermore, companies can suffer reputational damage without negative media coverage. If sensitive data is compromised, trust can be destroyed among core stakeholders without media involvement.

CYBER INSURANCE AS A SERVICE

Increasing interconnectivity means it is more important than ever for companies to review cyber security and resilience and consider the role of cyber insurance as part of their risk management. As the cyber threat evolves, so does the cyber insurance proposition, beyond just covering financial loss such as BI and restoration costs. For example, if an organization suffers a data breach it will need instant access to specialist lawyers, IT forensics and crisis management consultants to help mitigate the impact of an incident as it develops. Insurance provides this.

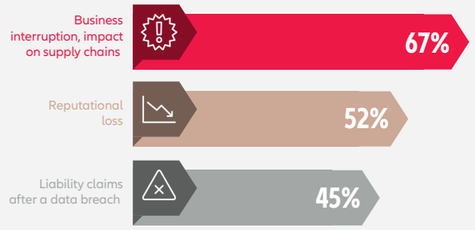
"Companies can't bury their heads in the sand. The sooner they respond the better the outcome. Companies that respond poorly to a cyber incident will see more of a long-term impact on their stock price than those that respond well," says Donavan.

WHICH BUSINESS RISKS ARE CURRENTLY MOST UNDERESTIMATED?



Source: Allianz Global Corporate & Specialty.
Figures represent the percentage of answers of all participants who responded (902).
Figures don't add up to 100% as up to three risks could be selected.

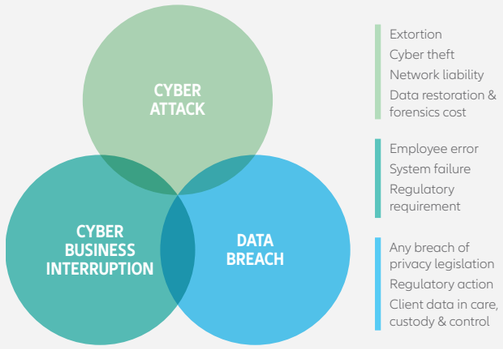
WHAT ARE THE MAIN CAUSES OF ECONOMIC LOSS AFTER A CYBER INCIDENT?



Source: Allianz Global Corporate & Specialty.
Figures represent the percentage of answers of all participants who responded (857).
Figures don't add up to 100% as up to three risks could be selected.

DIGI-DANGER: NOT JUST CYBER-ATTACKS

There are multiple threats to a company's digital presence



Source: Allianz Global Corporate & Specialty

GDPR: the most significant cyber risk development in 2018

Data protection security is back in the spotlight following huge breaches at Equifax and Uber in late 2017, which potentially exposed the data of 200 million people. The introduction of the **General Data Protection Regulation (GDPR)** across Europe in May 2018 will intensify scrutiny further. The GDPR introduces stricter procedures – such as the requirement to notify the regulator and data owners of a data breach – and significantly higher penalties for companies doing business in the EU who don't comply. Companies could be fined as much as 4% of global revenues, so more and larger fines can be anticipated. Demand for cyber insurance is also expected to increase, as companies bolster security in response.

"Compared with the US where laws are already strict and privacy regulation is continuously evolving, firms in Europe now also have to prepare for tougher liabilities and notification requirements," says **Emy Donavan, Global Head of Cyber at AGCS**. *"Many businesses are waking up to the fact they have potential vulnerabilities, and the realization that privacy issues create hard costs will emerge fairly quickly once GDPR is implemented. Being well prepared for a data breach will help reduce the reputational impact as well as the business interruption. Past experience has shown that the way in which an organization manages a breach has a direct impact on the cost. This will become even more the case under GDPR."*

1 Reuters, Merck cyber-attack may cost insurers $275 million: Verisk's PCS, October 19, 2017
2 Financial Times, Moller-Maersk puts cost of cyber-attack at up to $300m, August 16, 2017
3 Reuters, Hackers halt plant operations in watershed cyber-attack, December 14, 2017
4 MediaTenor, Enhancing risk management by helping companies shield and build their reputations

2018: 30%/2017: 24% (4)

3 MAJOR RISKS IN FOCUS
NATURAL CATASTROPHES

Uptick in activity begs the question: Is this a new "normal" of extreme weather? Allianz Risk Barometer respondents are concerned it is – and about the potential for larger losses

5-year risk rankings (% of responses and position):
2017 24% (4)
2016 24% (4)
2015 30% (2)
2014 33% (2)

Top risk in the following sectors:
- Engineering, Construction
- Entertainment & Media
- Marine & Shipping
- Oil & Gas
- Renewable energy

Approximately, $330bn in overall losses from natural catastrophes. Around $135bn in insured losses[1]. At least $90bn from the three category 4+ hurricanes – **Harvey, Irma, and Maria (HIM)** that wreaked havoc in September, making it the most active hurricane month on record[2] and 2017 one of the costliest seasons on record. Over $2bn dollars in insured losses from an earthquake in Mexico, also during September. Nearly $10bn worth of wildfire insurance claims in California alone through October[3]. Wherever you look, it doesn't take long to locate a startling statistic about natural catastrophe activity during 2017. And the numbers could get worse. Given the wide-ranging impact of HIM – from flood damage by Harvey in Houston to business interruption (BI) from record power outages in Puerto Rico caused by Maria – it may be some time before the final loss total is known.

Activity was not just confined to the Americas. Severe flooding events rocked Bangladesh, China, Sri Lanka, Peru and Zimbabwe. Killer mudslides devastated Columbia and Sierra Leone. Extreme wildfires tore across the Iberian peninsula and multi-seasonal drought conditions continued throughout the Mediterranean and parts of Africa and Australia, which was also hit hard by Cyclone Debbie in March. In the Philippines, Tropical Storm Tembin triggered floods and landslides on Christmas Day. If businesses had become complacent following a number of relatively quiet catastrophe years – by insurance standards at least – 2017 provided a wake-up call, ensuring natural catastrophe risk rises up the Risk Barometer to 3rd position in 2018.

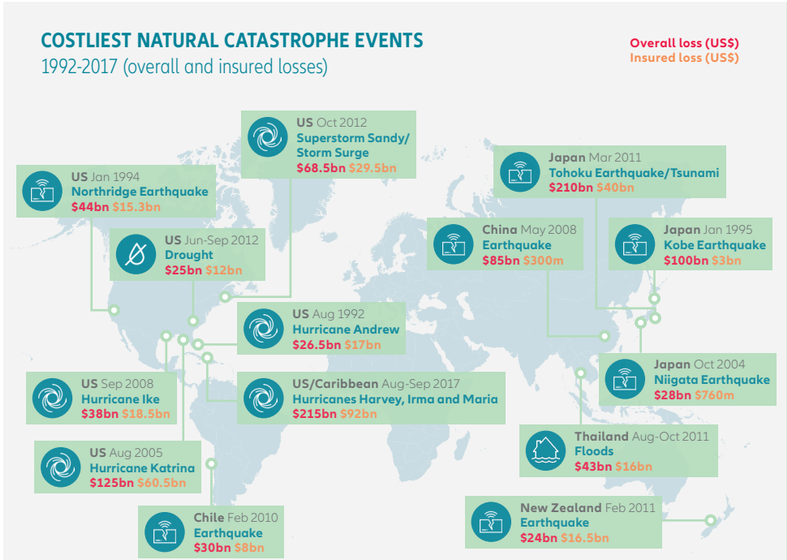
"Recent events have been a reminder of how significant the impact of natural catastrophes can be, both socially and economically," says **Ali Shahkarami, Head of Catastrophe Risk Research, AGCS**. *"As industries become leaner and more connected globally, it is becoming more and more clear that natural catastrophes can trigger or contribute to many other risks, such as business interruption or loss of market share, for example. This has certainly influenced the sustained attention on natural catastrophes in the Risk Barometer.*

"The impact of natural catastrophes goes far beyond physical damage to structures in the affected areas. They disrupt the normal dynamics of societal and industrial operations in the immediate regions affected and beyond, impacting a large variety of industries that might not seem affected at first glance."

CHANGING CLIMATE AND RAPID URBANIZATION

Respondents fear the 2017 natural catastrophe year could be a harbinger of things to come with many believing the intensity of natural catastrophes will increase in future due to the impact of a changing climate. Research shows there has been a 46% increase in weather disasters since 2000 and that 797 events were recorded in 2016 alone, resulting in $129bn of losses.[4] **Climate change/increasing weather volatility** (10th position) is a new entrant in the top 10 risks in 2018 *(see page 15)* and many scientists agree that changes in the climate and weather patterns have the potential to affect extreme events around the world in three primary ways – more intense windstorms, more incidences of heavy rainfall leading to flooding events and more severe drought episodes. Reinsurer Munich Re believes that although it cannot be attributed with any statistical significance, the changing climate already played a role in the 2017 hurricane season[5]. It also warns that the 2017 season looks like "a foretaste of the future" and that future projections of increased numbers of extreme storms may materialize in terms of a higher frequency of exceptional seasons such as 2004, 2005 and last year.

1 Munich Re NatCatService, Natural Catastrophe Review 2017
2 The Weather Channel, 2017 Atlantic hurricane season recap: 17 moments we'll never forget, November 28, 2017
3 California Department of Insurance, October wildfire claims top $9.4 billion statewide
4 The Lancet Countdown on health and climate change
5 Munich Re, The hurricane season 2017: a cluster of extreme storms



Sources: Munich Re NatCatService. **Graphic:** Allianz Global Corporate & Specialty.
Data as of March 2016, except Hurricanes Harvey, Irma and Maria – as of January 4, 2018.
Loss locations are for guidance only.

5 Steps to better natural catastrophe preparedness

If natural catastrophe risk management procedures are not in place, or have not been reviewed, the magnitude of such losses can increase significantly:

1. Test and update emergency preparedness plans
2. Determine what events to prepare for e.g. flood, wind, storm surge, and the exposures
3. Review and update business continuity plans
4. Understand the insurance policy – find any coverage gaps and plug them
5. Improve the site ahead of time to minimize event impact

↘ Windstorm checklist
↘ Flood checklist
↘ Earthquake checklist

The loss potential for businesses from future natural catastrophes is exacerbated by additional risk factors such as rapid urbanization – and the failure of development of sufficient infrastructure to keep pace with this – and greater interconnectedness, resulting in increasing contingent business interruption (CBI) and supply chain exposures. For example, there has been significant growth in population and development of commercial property in the US over the past decade. Modeler AIR Worldwide estimates the insured value of residential and commercial properties in coastal counties in the US now exceeds $13trn[6]. Values have increased 13% in three years.

"There are more people and more development in harm's way especially along the US coasts," says **Andrew Higgins, Technical Manager, Americas, Allianz Risk Consulting, AGCS**. *"In order to protect coastal communities, there need to be ample zoning laws to prevent unbridled overdevelopment, along with less concrete and more green space to allow tropical rains to properly drain. For example, some areas of Houston received about half of the amount of rain from Hurricane Harvey compared with a record-setting deluge in Nederland, Texas* (154cm/60.6 inches[7]*), but experienced much worse flooding. The difference is overdevelopment."*

NEW TOOLS FOR RAPIDLY-CHANGING RISK CONCENTRATION

In order to keep up with rapidly-changing risk concentration, insurers such as AGCS are using a variety of new catastrophe management tools and insurance solutions to monitor storms and assess natural catastrophe damages from events such as those in 2017. These tools include drones – used outdoors to assess roof wind damages and inaccessible locations, but also indoors to assess water damage in large facilities – and satellite technology and 3D imagery, to locate risks more quickly and more precisely.

"Currently we have several initiatives ongoing that combine state-of-the-art data analytics tools and the geographic information system (GIS) with the latest technologies on satellite imagery, big data and machine learning to provide advanced solutions that will significantly aid critical decision-making," explains Shahkarami. *"For example, this would allow us to have aerial images of impacted regions and potentially assess damage level to facilities immediately after a wildfire event or estimate the extent of flooding or damage to the top of the roofs of buildings after a windstorm. We live in exciting times from a technological perspective and are eager to utilize every tool available to better serve our customers."*

1,100+

Number of claims handled in 60 days by AGCS from 4 events – three hurricanes and a wildfire

6 AIR Worldwide, The Coastline at Risk: 2016 Update to the Estimated Insured Value of U.S. Coastal Properties
7 Washington Post, 60 inches of rain fell from Hurricane Harvey in Texas, shattering U.S. storm record, September 29, 2017

TOP BUSINESS RISKS: 4-10

4 MARKET DEVELOPMENTS

22% ▼ 2017: 31% (2)

Businesses are less concerned about this risk than 12 months ago, after a "special year" for multinationals in 2017, according to **Ludovic Subran, Global Head of Macroeconomic Research at Allianz**. The three economic superpowers (the US, Europe, and China) grew in sync, global trade rebounded, and markets offered excellent financial conditions and record low volatility; all in spite of heightened political and policy uncertainty. This alignment is expected to continue, albeit with caveats. With record amounts of cash on balance sheets, another M&A wave is expected in 2018, as increasing share buybacks cast doubt on the ability to grow organically in the face of the digital revolution. In addition, should markets and politics reconnect, volatility could potentially increase to mid-90s levels. Although bankruptcies around the world are stable, activity is up in the retail, services and construction sectors. Industries closest to the final consumer are first in line for disruption and are already impacted by price pressures.

5 CHANGES IN LEGISLATION AND REGULATION

21% = 2017: 24% (5)

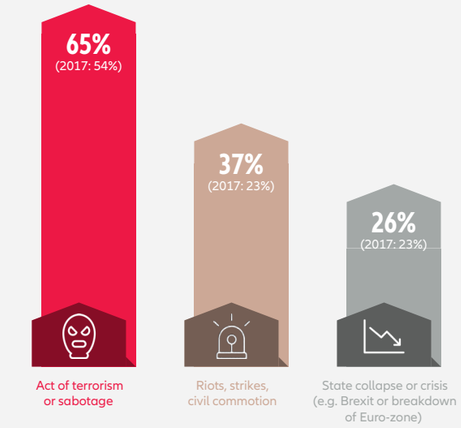
In 2017, only 404 new protectionist measures were taken globally, according to **Ludovic Subran, Global Head of Macroeconomic Research at Allianz**, half that of previous years. Yet protectionism is on companies' minds because the new barriers to trade came mainly from the US and affected China, showing the concentration of such impediments to trade are political. In 2018, the world will continue to be very fragmented. Global trade agreements and multilateral platforms are on the back burner, as economic and financial balkanization becomes the norm: the US-initiated tax war, uneven monetary and regulatory conditions between regions, and the politicization of currencies threaten capital flows. The top political risks continue to be about economic drivers, such as a fragmented Gulf region, as oil prices remain low and continued secession risks in Europe as economic imbalances prevail.

6 FIRE, EXPLOSION

20% ▲ 2017: 16% (7)

Analysis of more than 11,000 large industrial insurance industry claims by AGCS shows that fire and explosion incidents are the second major cause of loss for businesses overall. And the impact of the subsequent disruption to operations can often outweigh that of the physical damage caused. Fire and explosion incidents are the leading driver of business interruption insurance claims over a five-year period, with the average cost of a large incident totaling €1.7m ($2m). It is no wonder then that this risk continues to resonate with global respondents year after year – it also ranks second in the causes of business interruption companies fear the impact of most, after cyber risk. Fire and explosion is also the major peril for businesses in two countries – Burkina Faso and Togo – appearing in the Risk Barometer for the first time.

WHICH POLITICAL AND VIOLENCE RISKS ARE BUSINESSES MOST WORRIED ABOUT?



Source: Allianz Global Corporate & Specialty.
Figures represent the percentage of answers of all participants who responded (246).
Figures don't add up to 100% as up to three risks could be selected.

7 NEW TECHNOLOGIES

15% ▲ 2017: 12% (10)

The technological advances of the last decade are the main driver behind growing cyber exposures for businesses. No industry is untouched by the penetration of digitalization and the vast amount of information exchanged at all stages of the value chain. This interconnectivity enables growth, cost optimization and more flexible business models, closer to the final customer. Frequency of smaller losses may be reduced due to increased predictive maintenance, driven by real-time monitoring and data analytics. However, interconnectedness also poses significant risks related to inability to deliver products or services and may be accompanied by the potential for larger-scale losses from cyber-attacks and infrastructure breakdown. Increasingly, connected industries will experience new liability scenarios, ensuring this risk also ranks as the second most important business peril for the next 10 years *(see page 18)*, according to respondents.

8 LOSS OF REPUTATION OR BRAND VALUE

13% ▲ 2017: 13% (9)

Health and safety incidents, product recalls and data security breaches – in an age when a crisis can spread globally within minutes thanks to social media and interconnected supply chains, the risk of reputational damage from a multitude of sources has exploded exponentially. Almost a quarter of a company's value (24%) is estimated to lie in its brand[1]. Studies also suggest there is an 80% chance of a public company losing 20% of its equity value in any single month over a five-year period due to a reputational crisis[2]. No business is too small to be unaffected. Reputation can often be under-protected but insurance can provide tangible assistance to an intangible risk, such as funding for, and access to, crisis management experts. A professional response can make a difference. Research shows the share price of companies that effectively managed crises rose by over 10% the following year. Those which failed experienced a 15%+ drop[3].

9 POLITICAL RISKS AND VIOLENCE

11% ▼ 2017: 14% (8)

Businesses' perception of the threat posed by political risks and violence remains relatively unchanged year-on-year. However, respondents are more worried about terrorism. Businesses do not have to be the direct victim to feel the effects. If an attack occurs nearby the surrounding area may be closed, impacting operations. 2018 is expected to bring an increasing numbers of attacks in Western Europe and North America, according to **AGCS Head of Global Crisis Management, Christof Bentele**. The continued use of kinetic or low intensity attacks will dominate but there could also be further bombing incidents, like those seen in Manchester, UK and Brussels, Belgium recently, driven by returning IS fighters from the Middle East. Transportation infrastructure and locations with large groups of people, including retail, are likely main targets. Globally, a general trend of increased political activism can be anticipated, causing further disruption.

10 CLIMATE CHANGE/INCREASING VOLATILITY OF WEATHER

10% ▲ 2017: 6% (14)

The 2017 natural catastrophe year now ranks as the most expensive in history, with insured losses of $135bn[4], ending a run of relatively benign loss years – by insurance standards. Yet, overall, the frequency and severity of weather events is seen by many to be increasing. Between 2000 and 2016 there was a 46% increase in weather disasters with 797 "extreme" events recorded in 2016, research shows[5]. Finding a direct link between climate change and an increase in weather events is not straightforward. There are other factors behind record losses, such as rapid urbanization, and yet, clearly, the impact of a changing climate is an increasing concern for Risk Barometer respondents. It appears as a top 10 risk in 11 countries for the first time. Preparedness and risk mitigation can be the difference between businesses suffering a serious loss from a weather event and a catastrophic one.

1 Brand Finance Global 500 Report 2012 **2 and 3** Oxford Metrica/Aon Reputation Review 2012

4 Munich Re NatCatService, Natural Catastrophe Review 2017 **5** The Lancet Countdown on health and climate change

SME BUSINESS RISKS

Awareness of the cyber threat is soaring among small- and medium-sized businesses as the potential impact from data breaches and phishing attacks hits home. Fighting back poses a different set of challenges compared with larger companies

Collectively, small- to medium-sized (SME) business experts now account for almost half of Risk Barometer responses (47%). For medium-sized companies *(annual revenues between €250m and €500m)*, cyber incidents ranks as the top risk for the first time (39% of responses), while for small-sized companies *(annual revenues less than €250m)* it ranks as the 2nd major business risk (30% of responses)

"The jump that cyber incidents have taken in the past year – from 3rd to 1st for medium-sized companies and from 6th to 2nd for small-sized companies – is significant and reflects an uptick in the attention paid to data breaches both by SME companies and their insurance brokers," says **Vinko Markovina, Global Head of MidCorp, AGCS**.

"Awareness is growing, as the Risk Barometer results show, but many SMEs still underestimate their exposure and are not prepared for, or are able to respond to, an incident. This can be a fatal mistake."

As increasing numbers of cyber incidents occur and are reported, more evidence of its financial impact is available to SME-sized businesses. The impact can be catastrophic. Research shows that in in 2017, the average cost of a data breach in North America was $117,000 for SMEs[1], while other studies show that hackers have breached over 50% of small businesses, with these numbers up year-on-year[2].

SMEs can be vulnerable as many do not have sufficient revenue to afford their own IT departments or access to the knowledge and resources to protect themselves against evolving threats. They can be particularly susceptible to phishing attacks via email or fraudulent activity happening in their e-commerce storefronts.

Employing a Chief Information Security Officer (CISO) who can implement a comprehensive information security management system is considered a must in combatting the cyber threat but this can be costly and time-consuming and is often beyond the financial reach of many SMEs. However, AGCS has partnered with Silicon-Valley based software company Zeguro to implement a **"virtual CISO"** platform as part of its insurance coverage, which enables SMEs to access tailored security recommendations and training for employees, helping to reduce the overall risk of financial loss following an incident.

"Cyber insurance used to be a confusing and relatively expensive cover for SME-sized businesses. However, as coverage has become more available, affordable and easier to understand, we are seeing more demand," says Markovina. *"Activity around cyber will only accelerate in the SME space through 2018."*

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

↘ View the full risk rankings for 16 industry sectors

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

Rank		Percent	2017 rank	Trend
1	**Business interruption (incl. supply chain disruption)**	**33%**	2 (27%)	▲
2	Cyber incidents (e.g. cyber crime, IT failure, data breaches)	**30%**	6 (22%)	▲
3	Natural catastrophes (e.g. storm, flood, earthquake)	**28%**	4 (25%)	▲
4	Market developments (e.g. volatility, intensified competition / new entrants, M&A, market stagnation, market fluctuation)	**27%**	1 (32%)	▼
5	Changes in legislation and regulation (e.g. government change, economic sanctions, protectionism, Brexit, Euro-zone disintegration)	**22%**	3 (26%)	▼

Source: Allianz Global Corporate & Specialty. Figures represent how often a risk was selected as a percentage of all responses for that company size. Responses: 603. Figures don't add up to 100% as up to three risks could be selected.

Business interruption (BI) ranks as the top risk for small enterprises (33% of responses), up from 2nd (27%) year-on-year, and as the second most important peril for medium-sized companies, although this has been displaced by cyber incidents as the most important risk in 2018.

"It's no surprise that BI ranks prominently in the SME risk rankings, as threats are multiplying and the consequences cannot be underestimated," says **Vinko Markovina, Global Head of MidCorp, AGCS**. *"Supply chain disruption is just one element of BI risk that can impact SMEs. Maintaining sufficient on-hand inventory levels, avoiding geographic concentrations of suppliers, monitoring mergers and acquisitions among suppliers and avoiding production specialization that leads to outsourcing can all be crucial mitigation strategies in event of an interruption. If not managed effectively, the fall-out can quickly escalate."*

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

Rank		Percent	2017 rank	Trend
1	**Cyber incidents (e.g. cyber crime, IT failure, data breaches)**	**39%**	3 (29%)	▲
2	Business interruption (incl. supply chain disruption)	**37%**	1 (35%)	▼
3	Natural catastrophes (e.g. storm, flood, earthquake)	**32%**	5 (23%)	▲
4	Fire, explosion	**23%**	7 (17%)	▲
5	Market developments (e.g. volatility, intensified competition / new entrants, M&A, market stagnation, market fluctuation)	**21%**	2 (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: 516. Figures don't add up to 100% as up to three risks could be selected.

Four SME Risk Risers

Natural catastrophes
The record-breaking 2017 loss year has provided a wake-up call for small- and medium-sized businesses after a relatively quiet couple of years

Climate change
Small- (7th position) and medium-sized (8) businesses are more worried about its impact than larger corporations (>€500m annual revenue) for whom it doesn't appear in the top 10 risks

Political risks and violence
Medium-sized companies (10th position) are increasingly concerned about the indirect impact of terrorism and civil commotion events, which can keep customers away

Fire, explosion
Impact is much more of a concern for medium-sized companies where it ranks as 4th top risk. Fall-out can be terminal, destroying stock, halting production and interrupting cash flow.

1 Kaspersky Lab
2 Ponemon Institute, 2017 State of SMB Cybersecurity Report

FUTURE RISKS

Advancements in technology are changing the risk landscape irrevocably, representing both a boon and a challenge for businesses. On the one hand, technological innovation provides new ways to mitigate risk. On the other it creates new perils, which ranks as an increasing concern for Allianz Risk Barometer respondents

7

risk ranking for new technologies in the Allianz Risk Barometer, up from 10 in 2017

↘ View a position paper on autonomous machines

Autonomous machines. Artificial intelligence (AI). Smart factories and digitalized supply chains. The opportunities for businesses from deployment of new technologies are immense and wide-ranging. It is anticipated that increasing interconnection of buildings, factories and devices and better utilization of data and analytics, will enable greater productivity and more tailored customer offerings. Safety will be improved as human error – a leading cause of loss in many industries – is minimized due to automation of tasks. Autonomous machines can perform tasks in hazardous working environments, such as mines, reducing the risk of workplace injury, or in dangerous or inaccessible locations, improving disaster response and relief. Meanwhile, ongoing condition monitoring and use of "big data" analytics could significantly improve risk management, enabling better risk mitigation and prevention, more robust pre-disaster planning and even the ability to learn from near-misses.

NEW VULNERABILITIES

However, even outside of some of the major ethical and societal concerns that surround our growing reliance on new technology, such as the potential eradication of jobs and its use in war or influencing the views of the public via **"fake news"**, there are a growing number of new risks that businesses have to face.

In today's connected industries of smart factories and digitalized supply chains, where intangible assets such as data, networks, customer relationships and intellectual property can represent the major source of corporate value, more is at stake if things go wrong. Unintentional errors or unexpected consequences of applications of new technology can quickly impact consumer trust and cause reputational harm, as data privacy risks become more prominent and exposure to business interruption risk is compounded.

Vulnerability of connected systems to system failure or hacking and other malicious cyber acts such as extortion and espionage will increase further in future. According to a recent report by Lloyd's and Cyence Risk Analytics[1], a malicious hack that takes down a cloud service provider could cause estimated losses in excess of $50bn for an extreme event.

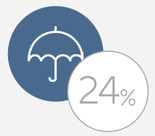
Loss frequency may be reduced due to automation minimizing the human error factor.

1 Lloyd's and Cyence Risk Analytics, Counting the cost: Cyber exposure decoded

WHAT ARE BUSINESSES' TOP THREE RISKS FOR THE LONG-TERM FUTURE? (10+ YEARS)

1. Cyber incidents

2. New technologies



3. Climate change/ increasing volatility of weather

Source: Allianz Global Corporate & Specialty. Figures represent the percentage of answers of all participants who responded (1,911). Figures don't add up to 100% as up to three risks could be selected.

However, this may be replaced by the potential for larger scale losses. The same programming error or hacker attack could be replicated on numerous machines. Or one machine could repeat the same erroneous activity several times, leading to an unforeseen accumulation of losses and to difficulties in clearly identifying what went wrong.

"A systemic malfunction of autonomous machines controlling critical infrastructure (IT networks, power supply) could significantly affect our interconnected global economy and society," says **Michael Bruch, Head of Emerging Trends at AGCS**. *"And will there really be less human error or is there only a shift in the type of human error, moving from the operator/driver to the software programmer of an algorithm or data analyst, which is actually the manufacturer?"*

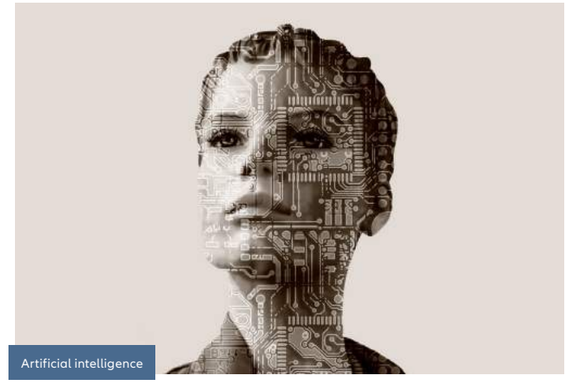
NEW LIABILITY SCENARIOS AND AN INCREASE IN PRODUCT RISK

Businesses will face new liability scenarios caused by this possible shift of responsibility from human to machine, and therefore to the manufacturer or its suppliers, with assignment and coverage of liability becoming more challenging. Digital products are complex. Therefore, liability may arise from a product defect, from 3D-printing for example, or could be traced back to a user error. It could even result from communication errors between two machines, machines and sensors or between machine and infrastructure.

Technology will also likely become a bigger driver of product recalls in future, whether due to cyber security vulnerability or untested AI, nanotechnology or biotechnology advances.

"Cyber risk is currently underestimated for product recall despite there having been recalls because of cyber security vulnerabilities in cars and cameras," says Bruch. *"Recalls involving emerging technologies could also be even larger and more complex than today. If a series of accidents raises safety concerns for the AI technology behind driverless cars, it could trigger a massive recall across different manufacturers and countries."*

In future, transition periods where humans and autonomous machines interact and coexist will also likely result in a period of intensified risk. For example, when both (fully or partially) autonomous connected vehicles are on the roads together with conventional ones, a higher rate of accidents is anticipated before a breakthrough in road safety is achieved.



Artificial intelligence

Smart factories and digitalized supply chains

The internet of things

Autonomous machines

Photo: Grendelkhan/Wikimedia Commons

Allianz Global Corporate & Specialty business scope

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. Insurance product lines covered include:

- Alternative Risk Transfer
- Aviation (including space)
- Energy
- Engineering
- Entertainment
- Financial Lines (including directors' and officers' [D&O])
- Liability
- Marine
- Mid-Corporate
- Property

Credits

Contributors:
Christina Hubmann, Heidi Polke-Markmann, Patrik Vanheyden

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

Design:
Kapusniak Design

Images:
Adobe Stock

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

CONTACT US

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

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

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

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

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

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

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

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 #ARB2018** and

LinkedIn

www.agcs.allianz.com

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

January 2018