(=) 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."*

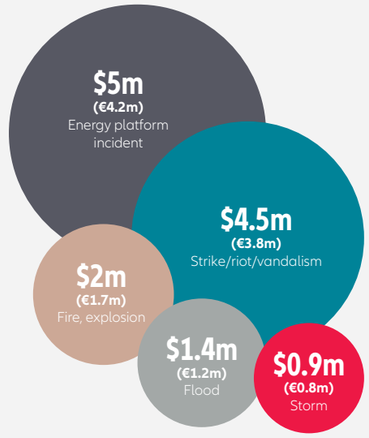
The threats don't stop there. In today's uncertain political and business landscape, where the prospect of an abrupt change of rules disrupting business models is an increasing concern, a withdrawal of regulatory approval or product license is another potential BI risk.

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

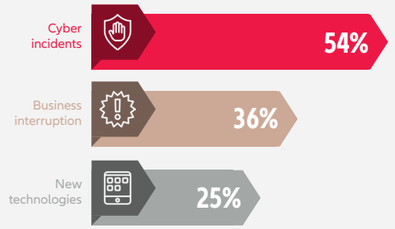
Cyber incidents aren't just caused by hackers. Technical failure or malicious or innocent employee action is often to blame. Whatever the cause, reputational damage is irrevocably linked. According to reputation analysis and research institute, MediaTenor, 75% of all companies which suffer a cyber-attack 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.

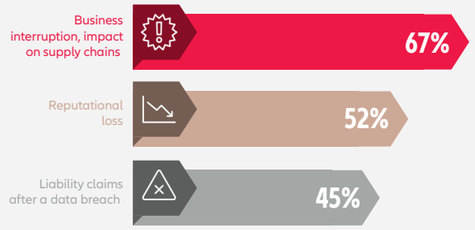
"Companies can't bury their heads in the sand. The sooner they respond the better the outcome. Companies that respond poorly to a cyber incident will see more of a long-term impact on their stock price than those that respond well," says Donavan.

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.

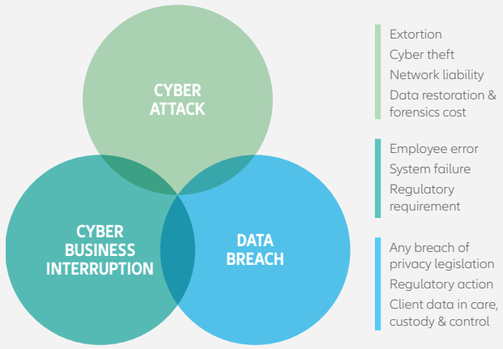
WHAT ARE THE MAIN CAUSES OF ECONOMIC LOSS AFTER A CYBER INCIDENT?



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