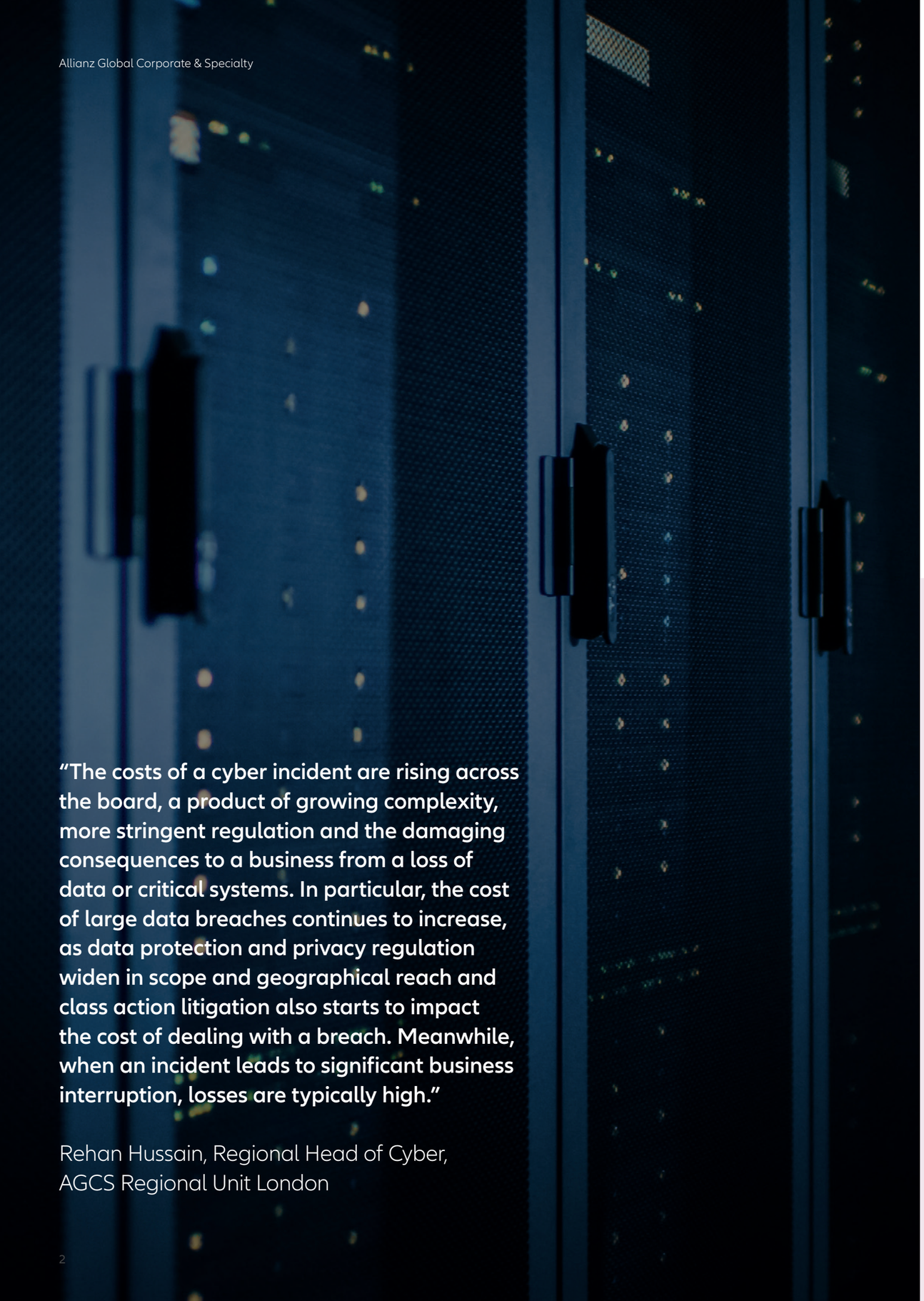
Allianz

Cyber risk trends to watch

CORONAVIRUS AND BEYOND

AGCS.ALLIANZ.COM



"The costs of a cyber incident are rising across the board, a product of growing complexity, more stringent regulation and the damaging consequences to a business from a loss of data or critical systems. In particular, the cost of large data breaches continues to increase, as data protection and privacy regulation widen in scope and geographical reach and class action litigation also starts to impact the cost of dealing with a breach. Meanwhile, when an incident leads to significant business interruption, losses are typically high."

Rehan Hussain, Regional Head of Cyber, AGCS Regional Unit London

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

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

Allianz Risk Barometer 2020 risk in focus: **Cyber incidents**

Global ranking history (position, % of responses)

- 2020: 1 (39%)
- 2019: 2 (39%)
- 2018: 2 (39%)
- 2017: 3 (39%)
- 2016: 3 (39%)
- 2015: 5 (39%)

Top risk in the following countries

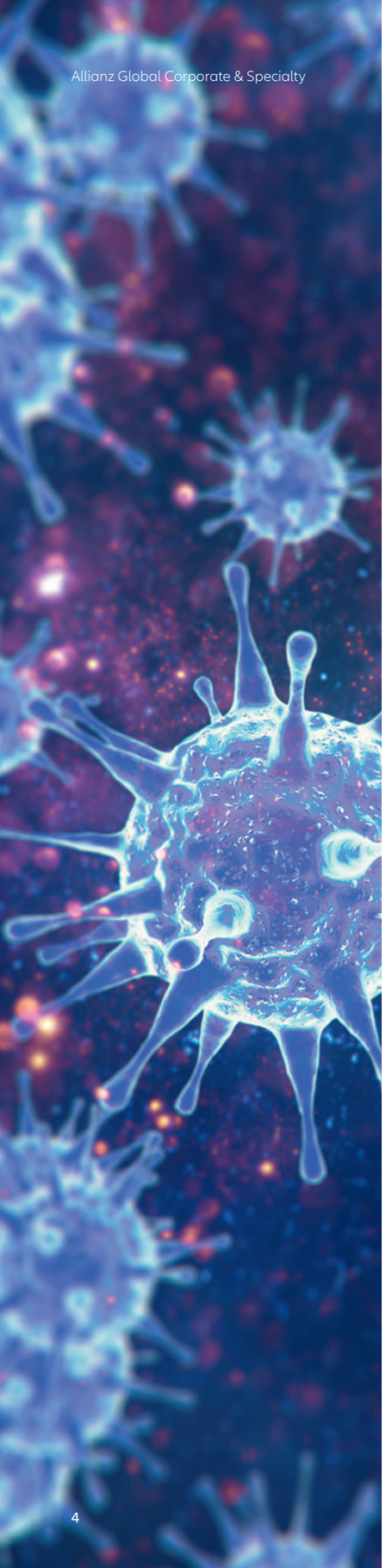
- Austria
- Belgium
- France
- India
- Malaysia
- South Africa
- South Korea
- Span
- Sweden
- Switzerland
- UK
- USA

Top risk in the following sectors

- Aviation
- Financial Services
- Government & Public Services
- Professional Services
- Technology
- Telecommunications

Allianz Risk Barometer 2020

The Allianz Risk Barometer is AGCS' annual report identifying the top corporate risks for the next 12 months and beyond, based on the insight of more than 2,700 risk management experts from 102 countries and territories. In 2020, for the first time ever, Cyber incidents ranked as the most important business risk globally. Awareness of the cyber-threat has grown rapidly in recent years, driven by companies increasing reliance on data and IT systems and a number of high-profile incidents. Seven years ago it ranked only 15th. Read more at www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer



Coronavirus

With many people working remotely because of the coronavirus outbreak, the **number of cyber incidents is increasing** as hackers, scammers and spammers look to exploit vulnerabilities in an attempt to steal valuable information.

Coronavirus is changing how people work and interact every day. Many companies have needed to expand their remote working capacity as a result of the outbreak – and usually at very short notice. In order to provide as many employees as possible with easy access to operating software and systems quickly, in some cases IT security standards may have had to be lowered or suspended, resulting in potential cyber security exposures for companies.

One consequence of potentially laxer security may be that **cybercriminals and hackers may find it easier to penetrate previous effectively protected corporate systems**, causing data breaches, cyber blackmail intrusions and IT system failures. It is estimated that anywhere between 50% and 90% of data breaches are caused or abetted by employees, be it by simple error or by falling victim of phishing or social engineering.

Unfortunately, the significant increase in home workers accessing the corporate network with a virtual private network (VPN) connection because of the coronavirus pandemic only exacerbates these risks, providing a perfect opportunity for cyber criminals, as recent events demonstrate only too well.

Coronavirus phishing scams with malicious links or attachments sent out by email or WhatsApp messages started circulating in January 2020 and their number has continued to increase since. The European Commission has said that cybercrime in the EU has risen since the outbreak began, while The World Health Organization (WHO) recently warned about suspicious email messages attempting to take advantage of the Covid-19 emergency[1] by stealing money and sensitive information from the public. In some countries, data shows that **the number of attempted cyber-attacks increased five-fold** between mid-February and mid-March. In April, Google detected and blocked more than 18 million malware and phishing emails and 240 million daily spam messages related to the pandemic in a single week[2]. In total, the tech giant blocks more than 100 million phishing emails each day.

[1] World Health Organization, Beware of criminals pretending to be WHO, 2020
[2] Google Cloud, Protecting Businesses Against Cyber Threats During Covid-19 And Beyond

A recent AGCS Risk Bulletin report suggested measures to consider for bolstering IT security in the home office, including:

- Keeping software up-to-date
- Activating virus protection and firewalls
- Being increasingly cautious about sharing personal data - online fraudsters increase their success rates by addressing victims individually
- Making sure web browsers are up-to-date
- Keeping passwords safe and changing them regularly. The general rule: the longer, the better
- Protecting confidential emails with encryption
- Only downloading data from trusted sources
- Making regular backups
- Turning off voice-activated smart devices and covering webcams when not in use
- Making clear distinctions between devices and information for business and personal use and not transferring work between the two. This will prevent unintentional information leakage
- Identifying all participants in online sessions
- Logging out when devices are no longer in use and keeping them secure
- Following security practices for printing and handling confidential documents
- Being careful with suspicious e-mails or attachments, especially if the sender is unknown.

For the full overview of IT security measures download the bulletin here: https://bit.ly/ARC-Coronavirus

Beyond coronavirus

Cyber trends to watch

What are the main causes of cyber incidents?

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

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

3. Errors or mistakes by employees

Source: Allianz Global Corporate & Specialty
Figures represent the percentage of answers of all participants who responded to the Allianz Risk Barometer 2020 (1,071). Figures don't add up to 100% as up to three risks could be selected

TREND

Data breaches larger and more expensive

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

Data breaches at hotel group Marriott in 2018 and credit score agency Equifax in 2017 were reported to have involved the personal data of over 300 million and 140 million customers respectively. Both companies faced numerous law suits and regulatory actions in multiple jurisdictions – the UK's data protection regulator intends to fine Marriott £100mn ($130mn) for the breach, among the earliest and largest fines under the EU's new privacy laws to date.

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

The General Data Protection Regulation (GDPR) rules that came into force across Europe in 2018 will likely bring further fines in 2020. The European Data Protection Board (EDPB) released a preliminary report[1] stating that of the 206,326 cases reported under the GDPR across 31 countries in the first nine months of its implementation, the national data protection agencies had only resolved around 50% of them. As shown above, as regulators have worked through this backlog, more fines of greater amounts have been recorded.

A mega breach now costs an average of $42mn[2], according to the Ponemon Institute, an increase of nearly 8% over 2018. For breaches in excess of 50 million records, the cost is estimated to be $388mn (11% higher than in 2018).

[1] European Data Protection Board, First Overview On The Implementation Of The GDPR And The Roles And Means Of The National Supervisory Authorities.
[2] IBM Security, Ponemon, Cost Of A Data Breach Report, 2019.

TREND

Ransomware brings increasing losses

According to the EU's law enforcement agency, Europol, ransomware is the most prominent cyber crime threat. Already high in frequency, incidents are becoming more damaging, increasingly targeting large companies with sophisticated attacks and hefty extortion demands. Five years ago, a typical ransomware demand would have been in the tens of thousands of dollars. Now they can be in the millions.

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

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

TREND

Business email compromise attacks result in billion dollar fraud

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

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

TREND

Litigation prospects rising

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

Data breach litigation in the US is a developing situation. A number of large breaches have triggered class actions by consumers or investors – in July 2019, Equifax reached a $700 million settlement for its 2017 mega breach. US courts have been battling the questions of "legal standing" – whether claimants have the right to sue – but the trend appears to be favoring plaintiffs. Statutory and regulatory changes could also facilitate compensation for data breaches. The California Consumer Privacy Act, for example, provides a mechanism for consumers to sue businesses and – in a first for the US – sets statutory damages for data breaches.

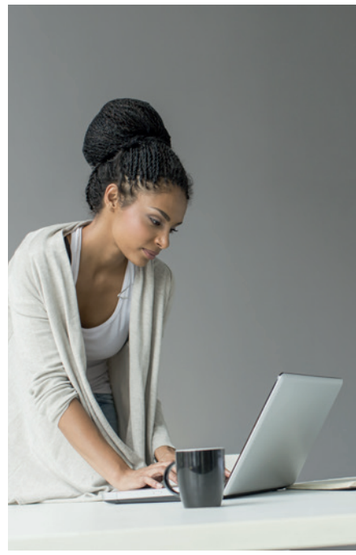
Outside the US, a number of countries have expanded group action litigation rights. For example, in Europe, the GDPR makes it easier for victims of a data or privacy breach to seek legal redress. In addition, claimant law firms and litigation funders are actively looking to bring class actions for data breaches in Europe and elsewhere – a class action against British Airways following its 2018 data breach was recently given the goahead in the UK courts. Consumer groups are also looking to test the GDPR and challenge some organizations' interpretation of the new law.

TREND

Political factors play out in cyber space

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

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



TREND

M&A can bring cyber issues

Cyber exposures have emerged as a hot topic in mergers and acquisitions (M&A) following some large data breaches. For example, the 2018 Marriott breach was traced to an intrusion in 2014 at Starwood, a hotel group it acquired in 2016. Even the best protected companies will be exposed if they acquire a company with weak cyber security or existing vulnerabilities. The acquiring firm could be liable for any damage from incidents which pre-date the merger.

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

What is the best approach to managing cyber risk and improving cyber resilience?

1 55%

Cyber risk is part of our overall enterprise risk management and is viewed as a key business risk

2 52%

Monitor and measure security and availability of systems through continuous vulnerability and risk assessments, remediation and sharing intelligence around cyber threats

3 45%

Regular staff information security trainings, awareness and anti-phishing campaigns

Source: Allianz Global Corporate & Specialty. Figures represent the percentage of answers of all participants who responded to the Allianz Risk Barometer 2020 (1,071). Figures don't add up to 100% as up to three risks could be selected.

Risk mitigation

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

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

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

Rehan Hussain, Head of Cyber, Regional Unit London, and Global Cyber Underwriter at AGCS

Contact us

The Allianz Global Corporate & Specialty (AGCS) UK Cyber Team bring their specialist knowledge and insights to help us deliver innovative, flexible solutions for our clients.

Stefania Davi-Greer
stefania.davigreer@allianz.com
Regional Head of Financial Lines

Rehan Hussain
rehan.hussain@allianz.com
Head of Cyber RUL

Michela Moro
michela.moro@allianz.com
Cyber Underwriting Manager

Daniel Lander
daniel.lander@allianz.com
Senior Cyber Underwriter

Lewis Bennett
lewis.bennett@allianz.com
Cyber Underwriter

About Allianz Global Corporate & Specialty

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

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

Worldwide, AGCS operates with its own teams in **31 countries** and through the Allianz Group network and partners in over 200 countries and territories, employing over 4,400 people. As one of the largest Property-Casualty units of Allianz Group, we are backed by strong and stable **financial ratings**. In 2020, AGCS generated a total of €9.3 billion gross premium 2020 globally.

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

Follow Allianz Global Corporate & Specialty on Twitter **@AGCS_Insurance** LinkedIn

For more information on AGCS visit **www.agcs.allianz .com**

Disclaimer & Copyright

Copyright© 2021 Allianz Global Corporate & Specialty SE. All rights reserved.

The material contained in this publication is designed to provide general information only. Whilst every effort has been made to ensure that the information provided is accurate, this information is provided without any representation or warranty of any kind about its accuracy and Allianz Global Corporate & Specialty SE cannot be held responsible for any mistakes or omissions.

Allianz Global Corporate & Specialty SE
Allianz House, 60 Gracechurch Street
EC3V 0HR, London, United Kingdom
Financial Conduct Authority Register 214374. Authorised by Bundesanstalt für Finanzdienstleistungsaufsicht.

Photos: Adobe Stock

February 2021