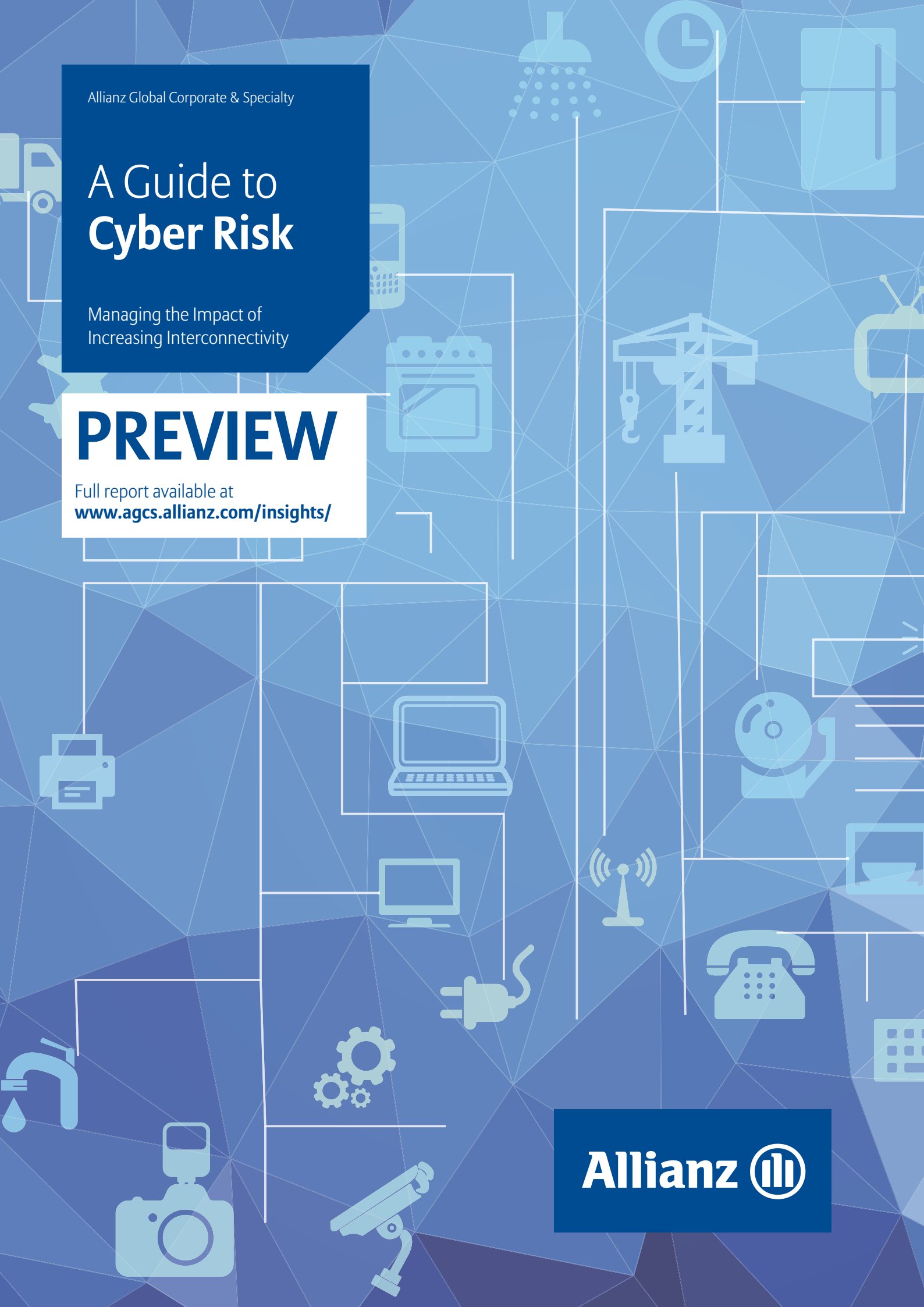
Allianz Global Corporate & Specialty

A Guide to **Cyber Risk**

Managing the Impact of Increasing Interconnectivity

PREVIEW

Full report available at
www.agcs.allianz.com/insights/



Allianz

Executive Summary

The cyber risk landscape today

$445bn

Estimated annual cost to the global economy from cyber crime[3]

$200bn+

Estimated annual cost to the world's largest four economies – the US, China, Japan and Germany

50%

The top 10 economies account for approximately 50%+ of cyber-crime costs

Increasing interconnectivity, globalization and **"commercialization"** of cyber-crime are driving greater frequency and severity of cyber incidents, including data breaches.

Data privacy and protection is one of the key cyber risks and related legislation will toughen globally. More notifications of, and significant fines for, data breaches can be expected in future. Legislation has already become much tougher in the US, Hong Kong, Singapore and Australia, while the European Union is looking to agree pan-European data protection rules. Tougher guidelines on a country-by-country basis can be expected.

Business interruption (BI), intellectual property theft and cyber-extortion – both for financial and non-financial gain – risk potential increasing. BI costs could be equal to – or even exceed – direct losses from a data breach.

Attacks by hackers dominate the headlines but there are many **"gateways"** through which a business can be impacted by cyber risk. Impact of BI triggered by technical failure is frequently underestimated compared with cyber-attacks.

Vulnerability of industrial control systems (ICS) to attack poses a significant threat. To date, there have been accounts of centrifuges and power plants being manipulated. However, the damage could be much higher from security sensitive facilities such as nuclear power plants, laboratories, water suppliers or large hospitals.

Cyber security and protection best practice

Cyber risk is the risk most underestimated by businesses according to the **Allianz Risk Barometer**[1] but there is no **"silver bullet"** solution for cyber security.

In addition to damages paid due to loss of customer data and impact of BI, loss of reputation can be a significant cause of economic loss for businesses after a cyber incident.

Monitoring tools, improved processes and greater employee awareness can help companies to be more prepared.

Businesses need to identify key assets at risk and weaknesses such as the "human factor" or overreliance on third parties. Employees can cause large IT security or loss of privacy events, either inadvertently or deliberately.

Businesses need to create a cyber security culture and adopt a **"think-tank"** approach to tackling risk. Different stakeholders from the business need to share knowledge. Implement a crisis or breach response plan. Test it.

Cyber risk is constantly evolving. **"Hidden risks"** can emerge. For example, businesses should consider how merger and acquisition **(M&A)** activity and changes in corporate structures will impact cyber security and holding of third party data in particular.

Companies need to make decisions around which risks to avoid, accept, control or transfer.

All $ US$ unless stated

1 *Allianz Risk Barometer surveys over 500 risk managers and experts from 40+ countries.*

Cyber risk and insurance – future trends and growth

The standalone cyber insurance market will continue to evolve but development will bring challenges, with many concepts and wordings yet to be tested, potentially resulting in litigation. This is not unusual with new products and can improve risk knowledge.

Education – both in terms of businesses' understanding of exposures and underwriting knowledge – must improve if insurers are to meet growing demand. Other challenges exist around pricing, modeling of risk aggregation and incidents resulting in physical damage.

The cyber insurance market is currently estimated to be worth around **$2bn** in premium worldwide, with US business accounting for approximately 90%. Fewer than 10% of companies are thought to purchase cyber insurance today. However, the cyber insurance market is expected to grow by double-digit figures year-on-year and could reach **$20bn+** in the next 10 years.

Growth in the US is already underway, driven by data protection regulation. Legislative developments and increasing levels of liability will help growth accelerate elsewhere, as will a growing number of small- to medium-sized enterprises **(SMEs)** seeking cover.

Sectors holding large volumes of personal data, such as healthcare and retail, or those relying on digitalized technology processes, such as manufacturing and telecommunications, are most likely to buy cyber insurance at present. However, there is growing interest among financial institutions and the energy, utilities and transport sectors, driven by the increasing perils posed by interconnectivity.

Data protection and liability risks dominate the cyber landscape today. Impact of BI from a cyber incident and further development of interconnected technology will be of increasing concern to businesses over the next decade and will spur insurance growth.

Businesses are also exposed to cyber risk through supply chains and, increasingly, will need to consider the impact of an incident in this area, such as the liability they could face if they cannot deliver their products or lose customer data, as well as the costs to resolve such issues. Companies will increasingly look to extend protection to their supply chains.

Emerging risks: impact of technology

"The Internet of Things" will have an increasing influence on the world in which we live and businesses operate. Estimates suggest as many as a trillion devices could be connected by 2020. New technologies create new vulnerabilities. Cyber criminals could exploit this increase in interconnectivity.

Businesses are driven by real-time data. Any interruption of the process chain – even for a minute – could cause a severe business interruption, impacting the balance sheet.

As technology evolves, older devices that remain in use could also create vulnerabilities, especially where they rely on outdated operating systems and unsupported software.

The use of outsourced services and storage – such as the **cloud** – brings risks, as well as benefits. One issue at a cloud provider could result in large BI and data breach losses for many.

The prospect of a catastrophic cyber loss is becoming more likely. An attack or incident resulting in a huge data loss or BI – and the subsequent reputational damage – could put a large corporation out of business in future.

A successful attack on the core infrastructure of the internet; for example main protocols such as Border Gateway Protocol (BGP) or Domain Name System (DNS), could be devastating[2].

A major cyber-attack or incident involving an energy or utility company could result in a significant outage, physical damage, or even loss of life in future, while a cyber war between two countries could disrupt internet services around the world.

Interest in protecting critical infrastructure is likely to see governments becoming increasingly involved in cyber security, resulting in greater levels of scrutiny and liability.

2 *Cyber Security In An Interconnected World: Recent Critical Events In A Nutshell, Allianz Group Economic Research*
3 *Net Losses: Estimating the Global Cost of Cyber-Crime, CSIS/McAfee*

Contents

The Cyber Risk Landscape Today
Increasing interconnectivity and "commercialization" of cyber-crime are driving greater frequency and severity of incidents.

Cyber Security and Protection Best Practice
Businesses must understand how cyber risk impacts their operations, how it can be mitigated and then determine their own risk appetite.

Evolution and Growth of Cyber Insurance
Cyber insurance is no replacement for robust IT security, but it can help to mitigate the impact of a number of different cyber incidents. However, challenges lie ahead.

Future Cyber Trends
Awareness of broader cyber risks will spur rapid insurance growth. As technology becomes more engrained in everyday life and business new perils will emerge.

Emerging Cyber Risks: Impact of Technology
Estimates suggest a trillion devices could be connected by 2020. The cyber risk landscape of tomorrow will look very different to that of today.

Media Contact

Heidi Polke-Markmann
Phone: +49.89.3800.14303
heidi.polke@allianz.com

About Allianz Global Corporate & Specialty

Allianz Global Corporate & Specialty (AGCS) is the Allianz Group's dedicated carrier for corporate and specialty insurance business. AGCS provides insurance and risk consultancy across the whole spectrum of specialty, alternative risk transfer and corporate business: Marine, Aviation (incl. Space), Energy, Engineering, Entertainment, Financial Lines (incl. D&O), Liability, Mid-Corporate and Property insurance (incl. International Insurance Programs).

Worldwide, AGCS operates in 28 countries with own units and in more than 160 countries through the Allianz Group network and partners. In 2014 it employed more than 3,500 people and provided insurance solutions to more than half of the Fortune Global 500 companies, writing a total of €5.4bn gross premium worldwide annually.

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

For more information please visit **www.agcs.allianz.com** or follow us on **Twitter @AGCS_Insurance**, **LinkedIn** and **Google+**.

View the full report at **http://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf**