Allianz Global Corporate & Specialty

Embargoed until 00:01 hrs CET, Wednesday September 9, 2015

Press Release

Businesses must prepare for new generation of cyber risks

- Allianz report highlights that cyber risks are evolving far beyond privacy or reputational issues.
- Global cyber insurance market forecast to grow to over $20 billion by 2025.
- Interconnectivity of devices and businesses drives new risk exposures with business interruption a key vulnerability, and catastrophic scenarios a possibility.
- Complexity of risk means businesses need to develop a cyber security culture with different stakeholders sharing risk management knowledge.

London/New York/Munich, September 9, 2015: Businesses must prepare for a new generation of cyber risks which are fast evolving, moving beyond the established threats of data breaches, privacy issues and reputational damage to operational damage, business interruption and even potentially catastrophic losses.

In a new report – A Guide to Cyber Risk: Managing The Impact of Increasing Interconnectivity – specialist insurer Allianz Global Corporate & Specialty (AGCS) examines the latest trends in cyber risk and emerging perils around the globe. Cyber risk is a major and fast-increasing threat to businesses with cyber-crime alone costing the global economy approximately $445 billion* a year, with the world's largest 10 economies accounting for half this total.

"As recently as 15 years ago, cyber-attacks were fairly rudimentary and typically the work of hacktivists, but with increasing interconnectivity, globalization and the commercialization of cyber-crime there has been an explosion in both frequency and severity of cyber-attacks," says AGCS CEO Chris Fischer Hirs. "Cyber insurance is no replacement for robust IT security but it creates a second line of defense to mitigate cyber incidents. AGCS is seeing

* Net Losses: Estimating the Global Cost of Cyber-Crime, CSIS/McAfee

increasing demand for these services, and we are committed to working with our clients to better understand and respond to growing cyber risk exposures."

Tougher regulatory regimes and new cyber perils

Increasing awareness of cyber exposures as well as regulatory change will propel the future rapid growth of cyber insurance. With fewer than 10% of companies currently purchasing cyber-specific policies, AGCS forecasts that cyber insurance premiums will grow globally from $2 billion per annum today to over $20 billion over the next decade, a compound annual growth rate of over 20%.

"Growth in the US is already underway as data protection regulations help focus minds, while legislative developments and increasing levels of liability will see growth accelerate in the rest of the world," says Nigel Pearson, who is globally responsible for cyber insurance at AGCS. "There is a general trend towards tougher data protection regimes, backed with the threat of significant fines in the event of a breach." Hong Kong, Singapore and Australia are among those looking at, or already enforcing, new laws and the European Union is looking to agree pan-European data protection rules. Tougher guidelines on a country-by-country basis can be expected.

Previously, attention has largely been focused on the threat of corporate data breaches and privacy concerns, but the new generation of cyber risk is more complex: future threats will come from intellectual property theft, cyber extortion and the impact of business interruption (BI) following a cyber-attack or from operational or technical failure; a risk which is often underestimated. "Awareness of BI risks and insurance related to cyber and technology is increasing. Within the next five to 10 years BI will be seen as a key risk and a major element of the cyber insurance landscape," says Georgi Pachov, cyber expert in AGCS's global property underwriting team. In the context of cyber and IT risks, BI cover can be very broad including business IT computer systems, but also extending to industrial control systems (ICS) used by energy companies or robots used in manufacturing.

Connectivity creates risk

Increasing interconnectivity of everyday devices and growing reliance on technology and real-time data at personal and corporate levels, known as the 'Internet of Things', creates further vulnerabilities. Some estimates suggest that a trillion devices could be connected by 2020, while it is also forecast that as many as 50 billion machines could be exchanging data daily. ICS are another area of concern as a number of these still in use today were designed before cyber security became a priority issue. An attack against an ICS could result in

physical damage such as fire or explosion, as well as BI.

Catastrophic event

While there have been some very large data breaches, the prospect of a catastrophic loss is becoming more likely, but exactly what it will look like is difficult to predict. Scenarios include a successful attack on the core infrastructure of the internet, a major data breach or a network outage for a cloud service provider, while a major cyber-attack involving an energy or utility company could result in significant outage of services, physical damage or even loss of life in future.

Stand-alone cover

Allianz also predicts that the scope of cyber insurance must evolve to provide broader and deeper coverage, addressing business interruption and closing gaps between traditional coverage and cyber policies. While cyber exclusions in property and casualty policies are likely to become commonplace, standalone cyber insurance will continue to evolve as the main source of comprehensive cover. There is growing interest among the telecommunications, retail, energy, utilities and transport sectors, as well as from financial institutions.

Education – both in terms of businesses' understanding of exposures and underwriting knowledge – must improve if insurers are to meet growing demand. In addition, as with any other emerging risk, insurers also face challenges around pricing, untested policy wordings, modeling and risk accumulation.

Responding to cyber risk

The AGCS report highlights steps companies can take to address cyber risk. Insurance can only be part of the solution, with a comprehensive risk management approach being the foundation for cyber defense. "Once you have purchased cyber insurance, it does not mean that you can ignore IT security. The technological, operational and insurance aspects of risk management go hand in hand," explains Jens Krickhahn, expert for cyber & fidelity at AGCS Central & Eastern Europe. Cyber risk management is too complex to be the preserve of a single individual or department, so AGCS recommends a 'think-tank' approach to tackling risk whereby different stakeholders from across the business collaborate to share knowledge.

In this way, different perspectives can be challenged and alternative scenarios considered: for example, these might include the risks posed by corporate developments such as

mergers and acquisitions or by the use of cloud-based or outsourced services. In addition, cross-company involvement is essential to identify key assets at risk and, most importantly, to develop and test robust crisis response plans.

###

For more information and to download the full report please go to:
http://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf

For AGCS Cyber insurance products visit http://www.agcs.allianz.com/services/financial-lines/cyber-insurance/

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 €5,4 billion 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+.**

Cautionary Note Regarding Forward-Looking Statements

The statements contained herein may include statements of future expectations and other forward-looking statements that are based on management's current views and assumptions and involve known and unknown risks and uncertainties that could cause actual results, performance or events to differ materially from those expressed or implied in such statements. In addition to statements which are forward-looking by reason of context, the words "may", "will", "should", "expects", "plans", "intends", "anticipates", "believes", "estimates", "predicts", "potential", or "continue" and similar expressions identify forward-looking statements.

Actual results, performance or events may differ materially from those in such statements due to, without limitation, (i) general economic conditions, including in particular economic conditions in the Allianz Group's core business and core markets, (ii) performance of financial markets, including emerging markets, and including market volatility, liquidity and credit events (iii) the frequency and severity of insured loss events, including from natural catastrophes and including the development of loss expenses, (iv) mortality and morbidity levels and trends, (v) persistency levels, (vi) the extent of credit defaults, (vii) interest rate levels, (viii) currency exchange rates including the Euro/U.S. Dollar exchange rate, (ix) changing levels of competition, (x) changes in laws and regulations, including monetary convergence and the European Monetary Union, (xi) changes in the policies of central banks and/or foreign governments, (xii) the impact of acquisitions, including related integration issues, (xiii) reorganization measures, and (xiv) general competitive factors, in each case on a local, regional, national and/or global basis. Many of these factors may be more likely to occur, or more pronounced, as a result of terrorist activities and their consequences.

The matters discussed herein may also be affected by risks and uncertainties described from time to time in Allianz SE's filings with the U.S. Securities and Exchange Commission. The company assumes no obligation to update any forward-looking statement.