Swiss Re
Institute

News release

Despite its complexities, insurers and companies can get to grips with cyber risk, Swiss Re *sigma* says; official launch Swiss Re Institute

- The potential costs of cyber-attacks are escalating rapidly; cyber security and resilience are a growing concern for firms
- A dedicated cyber insurance market is developing fast, but the scale of cover is still relatively modest
- Product & process innovations, and Big Data and smart analytics, will help foster improved cyber insurance solutions
- Governments can play an important role in boosting cyber resilience
- This is the first report published by the Swiss Re Institute, which officially launches today

Zurich, 1 March 2017 – Cyber risk is a growing concern for businesses, with recent attacks demonstrating that the costs of a cyber breach can escalate well beyond managing the fallout of lost or corrupted data. Swiss Re's latest *sigma* report "Cyber: getting to grips with a complex risk", says businesses need to do much more to integrate cyber security into their risk management programmes. Initiatives to boost cyber resilience are underway. A dedicated cyber insurance market is developing rapidly, but so far the scope of cover is modest relative to potential exposure. Product and process innovation and also advanced analytics will help foster improved cyber insurance solutions and extend both the boundaries of insurability and reach of cover. Ultimately, some cyber risks, especially those related to extreme catastrophic loss events, may be uninsurable.

Recent high-profile cyber-attacks increasingly demonstrate that the costs of a cyber security breach extend beyond managing the fallout of lost or corrupted data. Firms must now factor in the potential damage to their reputation, physical and intellectual property, and also disruption to business operations. The increasing scope and magnitude of potential costs associated with cyber-incidents reflect the ever-evolving cyber risk landscape, which in turn is being shaped by three main dynamics:

Darren Pain, Zurich
Telephone +41 43 285 2504

Kurt Karl, Armonk
Telephone +1 914 828 8686

Jonathan Anchen, Bangalore
Telephone +91 80 4900 2650

Investor Relations, Zurich
Telephone +41 43 285 4444

Swiss Re Ltd
Mythenquai 50/60
P.O. Box
CH-8022 Zurich

Telephone +41 43 285 2121
Fax +41 43 285 2999

www.swissre.com
@SwissRe

- the growing speed and scope of digital transformation;
- the widening sources of vulnerability from hyper-connectivity, with the rapid spread of, for example, internet-enabled devices and cloud computing;
- and the growing sophistication of hackers alert to the potential economic gains from successful cyber-attacks.

Despite increased awareness of the dangers, firms are generally ill-prepared to cope with cyber risks. Relatively few firms have integrated cyber security into their mainstream risk management. Regulation could be a catalyst for change with legislation coming into force in many jurisdictions requiring firms to build enhanced data protection safeguards. As a result, "firms – large and small – need to invest more in cyber security architecture to develop robust pre-and post-loss risk management capabilities," says Swiss Re Chief Economist Kurt Karl.

Managing a complex risk

Many firms are looking to transfer cyber risks to third parties better-placed to absorb them. "A dedicated cyber insurance market is developing, and an increasing number of insurers are looking to write more business in this specialty line," Kurt Karl continues. Dedicated cyber insurance typically provides core protection against data and network security breaches and associated losses, with capacity limits in the market today ranging from around USD 5 million to USD 100 million. However, some significant cyber-related risks remain largely uninsured and the scale of existing cover is modest relative to companies' overall potential exposures.

A key constraint on the development of insurance solutions is linked to the intrinsic nature of cyber risks. They are complex and difficult to quantify, especially given the fast-changing technological environment and lack of historical cyber-related claims data from which to extrapolate information about possible future losses. Insurers and risk analytics vendors are experimenting with different approaches to cyber risk modelling, including deterministic scenario analyses and probabilistic models, in an attempt to estimate the potential losses of cyber events. The experience of other perils, such as natural catastrophes, offers hope that models will continually improve as understanding of the fundamental risk drivers develops and more data about cyber losses becomes available.

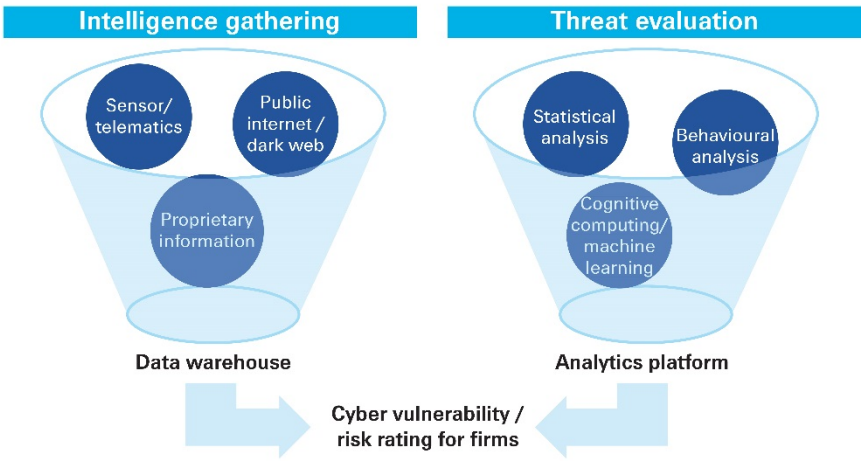
Product and process innovation

In the meantime, product and process innovation in insurance and other risk transfer mechanisms will play an important role in upgrading cyber risk management capabilities. A crucial factor influencing the pace of innovation will be the capture and analysis of relevant data and threat intelligence needed to underwrite cyber risks accurately. There are ongoing industry developments to upgrade information collection and dissemination.

For example, various risk analytics vendors have built data schema that provide firms with a standardised approach to identify, quantify and report cyber exposure to insurers.[1] Similarly, the CRO Forum is promoting a common language and framework for firms to capture salient information about cyber incidents and vulnerabilities.

For their part, insurers are looking to develop less complex and more flexible insurance products. These include covers that can be tailored to small and medium-sized businesses, which have hitherto been underserved by insurance and are often less well placed to cope with cyber risks than larger firms. Further, some re/insurers are seeking partnerships with cyber security firms and data analytics vendors to fill knowledge gaps and scale up/provide additional services to their clients. More generally, advanced analytics can augment re/insurers traditional underwriting tools, and help them respond quickly to fast-changing underlying risk factors.

Figure 1: Smart analytics as a complementary underwriting tool



Source: Swiss Re Economic Research & Consulting.

Another way to increase overall loss-absorbing capacity for cyber risk is by developing investment vehicles that enable capital market investors to take some of the exposures. There are currently some initiatives to develop insurance-linked securities (ILS) that cover operational-type risks like cyber. The ILS market for cyber risks remains nascent but could possibly grow.

[1] See, for example, "RMS Launches New Data Standard for Managing Cyber Insurance", *rms.com*, 19 January 2016, and *Verisk Cyber Exposure Data Standard and Preparer's Guide* , AIR, 2016.

Swiss Re Institute

Supporting role for governments

To expand the boundaries of insurability, companies will need to work with their insurers to create a sustainable market. Governments also have an important role in promoting cyber resilience, including measures to improve cyber information capture and diffusion, and setting laws and regulations about how cyberspace is used and protected. By reshaping incentives and increasing awareness of cyber threats, governments can further nudge the private sector into developing improved market-led solutions. Ultimately, however, the potential scale of losses from some cyber events could be too great for the private re/insurance sector to absorb, especially peak-loss events such as widespread disruption to critical infrastructure or networks which could lead to significant accumulated losses.

This *sigma* is the first to be published under the "Swiss Re Institute" banner. The Swiss Re Institute formally launches on 1 March 2017 with a mandate to build on Swiss Re's position as the thought leader in the industry, bringing together the firm's various high-quality research and outreach capabilities under one roof. The Swiss Re Institute will produce Swiss Re's research reports including *sigma*, the insurance industry's leading research publication.

Notes to editors

Swiss Re

The Swiss Re Group is a leading wholesale provider of reinsurance, insurance and other insurance-based forms of risk transfer. Dealing direct and working through brokers, its global client base consists of insurance companies, mid-to-large-sized corporations and public sector clients. From standard products to tailor-made coverage across all lines of business, Swiss Re deploys its capital strength, expertise and innovation power to enable the risk-taking upon which enterprise and progress in society depend. Founded in Zurich, Switzerland, in 1863, Swiss Re serves clients through a network of around 70 offices globally and is rated "AA-" by Standard & Poor's, "Aa3" by Moody's and "A+" by A.M. Best. Registered shares in the Swiss Re Group holding company, Swiss Re Ltd, are listed in accordance with the International Reporting Standard on the SIX Swiss Exchange and trade under the symbol SREN. For more information about Swiss Re Group, please visit: www.swissre.com or follow us on Twitter @SwissRe.

How to order this *sigma* study:

The English, German, French, and Spanish versions of the *sigma* No 1 /2017, *Cyber: getting to grips with a complex risk* are available electronically on Swiss Re's website: www.swissre.com/sigma

Printed editions of *sigma* No 1/2017 in English, German, French and Spanish are available. The printed versions in Chinese and Japanese will be available in the near future. Please send your orders, complete with your full postal address, to sigma@swissre.com