# Being prepared for the future

**An interview with Martin Kreuzer, Cyber Risk Specialist at Munich Re (Group) and former Domestic Intelligence Service member, about the global cyber landscape. 'Being prepared for the future means being prepared for cyber risks, exposures and their consequences.'**

***In many of today's lists of the most relevant risks, climate change and cyber often make it into the top three positions. What would you say are currently the most important risks to pay attention to?***
'It is very true that climate change and cyber risks are of the most importance for companies. In fact, business interruption and cyber incidents are the top global risks, even ahead of natural catastrophes.'

***What are some of the main forms of cyber risks and cyber losses that a modern business has to deal with or be aware of?***
'This is a loaded question that is ever-changing since we are constantly expanding coverage types based on new perils that come up. But to give you an idea of the broad range of risks, we at Munich Re focus on privacy breaches and network security interruptions to first and third parties, and on business interruptions resulting from cyber-attacks such as ransomware, distributed denial of service attacks, or phishing. Every year, we see an increase in business interruption losses due to cyber-attacks on supply chains and service providers. Since intruders are constantly looking for new and more sophisticated ways to infect software and hardware throughout the supply chain, we can expect these strikes to become more frequent and to have a more serious impact. This is why we consider BI insurance more important than ever.'

***... and the consequences of these events?***
'Well naturally, as attacks continue to increase globally, the demand for more comprehensive insurance covers and services rises too. As a consequence, we see this modern digital transformation as a clear demand for new solutions from the insurance and reinsurance industry.'

***So, this is changing the market overall.***
'Exactly. As the offering of cyber policies continues to grow worldwide, we are seeing the European and Asian markets quickly catching up to the US market. This increase in demand is opening up the insurance industry to a variety of new business opportunities. Yet realising this growth potential will require client managers, brokers, primary insurers and their sales forces to all acquire better training and a comprehensive understanding of cyber and silent cyber as well.'

***Could you elaborate on 'silent' cyber?***
'Being 100% cyber affirmative means being aware of cyber risks and exposures. Silent cyber refers to unassessed or unmeasured cyber exposures in traditional non-life business covers. Munich Re has made a huge effort to not only make silent cyber a key focus of our business but also, and more importantly, to deal with these risks that lie within traditional lines of business. Our strategy consists of understanding and assessing risks adequately and then providing bespoke insurable covers for them. Certain exposures, such as non-physical damage business interruption, should be excluded and shifted to stand-alone cyber covers. Although our preference would be to have cyber risk covered in stand-alone products, we recognise that a certain amount of risk will remain in traditional covers such as property damage and bodily injury.'

***Could you give some concrete examples of how companies could prevent themselves becoming victims of cyber-attacks and of where (re)insurance can help?***
'Well, it is first important to ensure that within the ever-changing cyber risk landscape, ultimately three things are under control. First, every company must do everything possible to make sure their IT infrastructure is technologically state of the art and that all security measures work after every update. Second is staying in charge of internal business processes and remaining transparent on how to deal with critical data and security standards. Why is this important? Because employee behaviour is one of the biggest loopholes for targeted attacks. And lastly, it must be clear what will happen in the event of an attack. After all, you can minimise the risk of being hacked, but not eliminate the risk. In the case of Munich Re, we focus on these three points of view as we dispatch our global cyber teams. It is also why we rely on a network of renowned external partners to complement our own knowledge and range of services. For example, we cooperate with IT security experts in order to offer solutions for our clients' entire value chain. Moreover, Munich Re avails of human resources ranging from Cyber Risk experts, dedicated cyber underwriters to cyber actuaries.'

## THE SKILLSET OF ACTUARIES MAKES THEM BEST PLACED TO DEVELOP THE MOST SUITABLE APPROACHES

***What contribution can actuaries deliver to the cyber topic?***
'Although actuarial textbooks are not yet filled with well-established techniques specific to quantifying cyber risk, the skillset of actuaries makes them best placed to develop the most suitable approaches. To do so, they must partner with relevant specialists such as IT security professionals, researchers, lawyers and underwriters. Actuaries are typically required to comply with a code of conduct. In the context of quantifying cyber risk, this means they must clearly articulate the level of 'model maturity' for their modelling approaches and ensure that all model users and stakeholders clearly understand the limitations of the approach in question.'

***Data (availability) is typically an issue when it comes to pricing a cyber-insurance product. Can you give some insight into how these products are priced?***
'As cyber is a relatively new area of insurance, many insurers have limited underwriting and loss experience to draw from for pricing purposes. However, there is a select group of multinational and US-focused insurers with 10+ years of experience and confidence in the levels of expected losses for their products. But attention must remain on the potential for bigger accumulation events than those seen so far, like Not-Petya, that all insurers need to estimate and incorporate into their pricing. This is an area of significant uncertainty.'

***In your opinion, were the most recent major cyber events a 'national' topic or are cyber events much more internationally driven?***
'Cyber, or digitalisation to put it more accurately, knows no limits or borders.'

***How do specific countries or even terrorists affect the overall cyber landscape?***
'Nowadays, it is widely acknowledged that cyberspace has become another domain of warfare. That may include cyber-attacks used for surveillance, economic espionage, sabotage or disinformation. This is all part of a what is called hybrid warfare, or at least a hybrid offensive approach. Despite all the differences, there is one common aspect between traditional domains of warfare and cyber-attacks: you can only defend yourself if you know how these attacks work. This means that a country that has built up significant resources to defend itself from cyber-attacks can also use these resources offensively.'

***What is Munich Re's outlook moving into 2020?***
'Together with our clients, we want to help people regard existing challenges less as threats and more as opportunities for new, long-term business. We are on the right track. The growth forecasts of the past years proved reliable. As long as our industry proceeds in a disciplined manner, this will continue to be a good source of business. Not only because of excellent growth prospects but also as a collective contribution towards fostering the economy.' ■

**Martin Kreuzer**
**Cyber Risk Specialist at Munich Re (Group)**
Martin Kreuzer is a specialist in the field of information security. Having studied at the German Federal University of Applied Administrative Sciences and Law, Martin worked for governmental structures in the sector of international public security and intelligence for more than a decade.

Being one of the very few examples in Germany that dare to quit a civil service career Martin joined Munich Re in January 2016. Within Corporate Underwriting Martin is responsible for information security and cyber risk management. Conducting risk assessments for special financial risks, delivering direct consulting and training for underwriting units and clients as well as the ongoing monitoring of cyber risks and cyber covers are major tasks in order to expand Munich Re´s leading role in the cyber insurance sector.