



**Swiss Re**  
Centre for Global Dialogue

## 11th CRO Assembly

Technological and societal  
change

Conference Report  
17–19 November 2015





Population-scale adoption of new digital technologies has produced novel working patterns and business models. Communities made up of providers and consumers of goods and services, organised through computer and smartphone contact, have emerged worldwide. The biggest, like Uber and AirBnB, already rival incumbent firms in terms of market capitalisation, and the new platforms are becoming a growing part of the world economy. Popular with their members, they encounter the resistance of groups feeling threatened by them. They also create and confront challenges regarding regulation, taxation and social funding.

Since advancing digitalisation entails collecting personal data, it raises questions of privacy and trust. Fundamental differences between the restrictive European approach to data protection and the more open American view complicate the issue. Cyber risk is on the rise as digitalisation increases, with cyber security gaining importance as a safeguard and an important enabler for growth.

The transformation of technology and work is accompanied by political and energy concerns and is occurring against a background of ageing populations and shrinking workforces. The associated difficulties regarding provision for old age and long-term care are daunting.

Will the insurance industry maintain its – still undisputed – relevance in the shifting landscape of technological and societal change? The challenges are tough. The property protection gap is enormous and growing; economic risks stem from Chinese reform, European political uncertainty and diverging central bank policies. Some products will be directly threatened. Motor insurance is likely to change radically, for example, when robocars come on the market and product liability replaces personal liability, with some manufacturers probably opting for self-insurance. The future offers opportunities for insurers too, especially in the retail area. New offerings, new partnerships and deployment of the latest technologies will be key to success.



**Patrick Raaflaub**  
Group Chief Risk Officer  
Swiss Re



**Anna Maria D'Hulster**  
Secretary General  
The Geneva Association



**Renzo Avesani**  
CRO Forum Chairman



# Table of contents

<b>Session 1: Digital disturbers and new business models</b>	4
Making insurance relevant for a digital age	4
The autonomous car: Who is liable?	6
Uber: the rise of real-time ride sharing	8
Cyber risk: a mutating threat, an evolving response	10
<b>Breakout sessions:</b>	
Insurance provision in a digital age: Disturbers and opportunities	12
<b>Session 2: Big data and the data protection challenge</b>	16
Autonomous driving cars and big data: how to maintain trust	16
Data privacy	18
<b>Breakout sessions:</b> Enhancing and protecting data usage in insurance	20
<b>Panel discussion:</b> Industry perspective on the data challenge	25
<b>Session 3: Changing societies and evolving risk landscapes</b>	28
Assessing the risk landscape in the energy sector	28
Digital health	30
<b>Breakout sessions:</b> Emerging societal risks	32
The future of work in the sharing economy	38
Ageing, demographics and societal change Forum	40
<b>11th CRO Assembly</b>	42
<b>Organisers</b>	43

### Making insurance relevant for a digital age

*Michel Liès, Group Chief Executive Officer, Swiss Re*

Digitalisation clearly presents a challenge to the insurance industry, but it is by no means the only one insurers face. The global property protection gap against natural catastrophe risk amounts to USD 68 billion annually and is growing. The mortality gap stands at USD 86 trillion, half of which is in Asia. To make headway in tackling these huge challenges, insurers have to convince governments of the need for national risk managers or even risk ministers. Creating this function would sharpen countries' awareness of the risks they face and of the available mitigation measures.

Asset risk will be high on CROs' agendas, with tail-risk scenarios such as China's economic reform slow-down, political uncertainty in Europe, and diverging central bank policies – a key risk given the financial markets' dependency on liquidity, all shaping the outlook. In fact, liquidity conditions are the wild card capable of amplifying any downside scenarios.

In this volatile situation, digitalisation will have a disruptive influence on insurance, but will present opportunities as well as challenges. There will be new underwriting models using big data and smart analytics. Machines will take some insurance decisions, rationally and objectively, and this should reduce the protection gap. Some products will be called into question, a prime example being motor insurance as autonomous vehicles come on the scene. These will probably elicit a move from personal to product liability, with the manufacturers of the software or of the cars assuming responsibility.

In the increasingly digitalised world, cyber attacks have cost various organisations huge sums, a notorious example being the DOS attack on Sony by the "Lizard Squad" in December 2014. Insurers need to improve their understanding of cyber threats and the risks associated with system malfunction. On the one hand, they must seize the underwriting opportunities offered by these risks, and on the other, although the insurance industry has not been a primary target of hackers, they must be able to protect the vast amounts of, partly sensitive, data in their charge. Regulators are increasingly incorporating cyber risk considerations into their policy, and fortunately the concerns of the regulators and the insurers seem to be well aligned in this area.

# The concerns of the regulators and the insurance industry are quite well aligned with regard to the digital economy and cyber risk.

*Michel Liès, Group Chief Executive Officer, Swiss Re*





Approaches to buying products like insurance differ with the age of the clients, ranging from conventional correspondence to texting, with further innovations inevitably to come. Insurers have to take this dynamic variety seriously and maintain an acute awareness of change. Greater use of the smartphone is an obvious way of shortcutting access to customers. Some industries have taken full advantage of the digital technologies, but insurance and reinsurance companies could be much more active in this respect, especially considering the enormous potential offered by the protection gap.

### The autonomous car: Who is liable?

*Brad Templeton, Networks & Computing Chair, Singularity University*

Autonomous cars, also called “robocars,” are a reality rather than science fiction. Conventional car manufacturers and others are working on their development, but with different approaches. The car companies are adding computers to cars, while digital corporations, like Google and Apple, are basically putting computers on wheels. Among car producers, the Germans have achieved the best results so far, but the overall development leader is Google with two million km of testing on normal roads to its credit. Apple is keeping its plans secret but seems to have an electric self-driving vehicle projected for 2019. Uber is technologically behind the others with its project, but as the number one in selling rides it might nevertheless be well positioned, since the long-term business of robocars may mainly be selling rides.

Autonomous vehicles are believed to be far safer than conventional cars and dramatically reduce the number of road accidents — KPMG estimates a drop of 80%. In addition to this life-saving factor, robocars are likely to radically change the way people live, fostering a trend away from car ownership to inexpensive mobility on demand. People will hire different vehicles for different purposes, from light single-seaters for urban travel to a variety of heavier vehicles. With self-refuelling capability, robocars will be able to use non-fossil fuels. They will also park themselves. These changes mean that CO<sub>2</sub> emissions will fall by millions of tons, and vast areas of freed-up parking space will become available for other (real-estate) purposes.

# The marriage of computers and cars will bring remarkable changes to the world, and certainly to the insurance industry.

*Brad Templeton, Networks & Computing Chair, Singularity University*





Some sectors will experience considerable upheaval as robocar technology gains ground. These include the vehicle manufacturers, energy, real estate, loans, car repairs and service and, of course, insurance. Personal liability in motor insurance is likely to become an issue of product liability, and among the companies developing autonomous vehicles, Google, Mercedes and Volvo have already stated that they will assume responsibility for accidents attributable to the software in their future robocars. Those vendors who decide to self-insure may still need to have reinsurance for regulatory reasons. Computer intrusion liability will be an issue since intrusion cannot be entirely eliminated. Because human drivers will still control certain autonomous vehicles for part of the time, there may have to be a regimen to underwrite the two ways in which the cars in question are driven. Car accidents occurring with a machine in control will differ greatly from accidents involving human drivers. Robocar incidents will be fully documented in 360° 3D and there should be no doubt about who is at fault. The issue will be why the software made a mistake, so that the problem can be fixed quickly and the particular mistake precluded for the future. It is essential to bear in mind that the car is becoming a digital product, and with the computer and software forming its most important component, it will be on the Moore's Law curve.

## Uber: the rise of real-time ride sharing

*Rasoul Jalali, General Manager, Uber*

*Jayne Plunkett, Head Casualty Underwriting Reinsurance, Member of Reinsurance Executive Committee, Swiss Re*

Mobility poses serious challenges for drivers and communities: pollution, congestion and the resulting delays and time lost, too much space taken up by car parks yet a lack of parking spaces from the drivers' point of view. In Switzerland, 4 million cars are used inefficiently, standing idle for 23 out of every 24 hours on average and having an average occupancy of 1.5 persons. Ride-sharing goes a long way towards solving the problems, allowing cars to be used more efficiently by increasing occupancy and reducing the level of vehicle ownership. Ride-sharing also yields faster travel times and constitutes a valuable adjunct to public transport.

This ongoing transport revolution was enabled by technological advance in the form of the smartphone. Customers use an app to contact Uber partner-drivers. When a driver accepts, the client is informed of that driver's name, the type of car and its licence plate number, as well as the driver's rating. After each trip, customers can rate the drivers and the drivers can rate the customers or "riders." The latter can request their rating, and many do. The transaction is cashless; the rider pays electronically and receives a receipt by email. Users have taken to this point-to-point transport system very eagerly, so that Uber has grown rapidly, creating an extremely dense network in some cities and achieving very low waiting times for the customers: two to three minutes in New York and San Francisco and five minutes on average in Zurich.



Ride-sharing allows cars to be used more efficiently and reduces road congestion, pollution and the demand for parking space.

Rasoul Jalali, General Manager, Uber

## Cyber risk: a mutating threat, an evolving response

*Richard Bach, Assistant Director for Cyber Security, UK Government's Department for Business, Innovation & Skills*

Three basic principles of cyber security are confidentiality, integrity and availability, where confidentiality means preventing the theft of data, integrity means preventing data corruption, thereby ensuring its accuracy, and availability means assuring that systems and information cannot be rendered unavailable. It is important to grasp that cyber security is about more than just information: it also includes information technology and operational technology (industrial control systems, process control, payment systems etc). Cyber attacks occur and are sometimes successful; it is essential for organisations to be able to detect them and mount an effective response. Implementing cyber security costs money, but the UK government, recognising that such security is attractive to businesses and forms a key enabler for economic growth, has doubled its five-year cyber security budget.

Considering risk to be a function of threat, vulnerability and impact, the factor most amenable to corrective action is vulnerability. Reducing that means reducing one's attack surface. The aim of the relevant protective activities is to achieve a state of cyber resilience, which the US Department of Homeland Security defines as "the ability to withstand and recover from deliberate attacks." By analogy with cars, organisations need virtual crumple zones, so that if a cyber attack cannot be warded off, at least a central zone containing the information assets is protected.

In the UK, the government-endorsed Cyber Essentials scheme provides companies of all sizes with guidance on basic cyber hygiene and good cyber security practice. Key to the success of the scheme is engaging the boardroom. One important element of this is to quantify the potential losses associated with cyber risk, because top management reacts vigorously to numbers, and these can be alarming even for SMEs. A further government scheme centres on cyber risk insurance. Participating insurers include the Cyber Essentials accreditations as part of their risk assessment for SMEs. The government's overall goals are to help the insurance industry establish cyber insurance as part of firms' cyber tool-kits and to consolidate London's position as the centre for cyber-risk management. Working together with the insurance

# We must prepare for, detect and mount an effective response to cyber attacks.

*Richard Bach, Assistant Director for Cyber Security, UK Government's Department for Business, Innovation & Skills*





industry, the UK government intends to establish a forum for data and insight exchange and policy discussions. The insurance sector will monitor market capacity and the need for a cyber risk pool. A further aim is to promote the cyber capabilities of the London insurance market to key countries worldwide. A “Cyber Re” facility has been suggested, but the UK government is currently against this, considering that the estimated maximum global exposure to a single event should be well within the market’s capacity to absorb it.

## Breakout sessions

### Insurance provision in a digital age: Disturbers and opportunities

#### 1. CRO Forum: The smart factory



*Marcia Cantor-Grable, Group Risk, Director – Emerging Risk and Regulatory Developments, Prudential*

Smart manufacturing or Industry 4.0 describes the convergence of innovative technologies, methods, materials and products that will transform life, business and the global economy. The term 'Industry 4.0' comes from the German government's strategy for technological development, on which it is spending EUR 40 billion per year until 2020. However, the development is taking place worldwide, as the Internet of Things becomes the Industrial Internet of Things, the catalyst for Industry 4.0. As technology advances, decision-making starts to move away from people to machines, and the development is underpinned by major innovations, including automation, robotics, autonomous mobility, machine-to-machine communication, big data and smart analytics, and 3D printing. This will optimise industrial processes with increased efficiency, a lower rate of breakdowns, and lower operating costs. It will also bring about profound change in many areas of life: the way we produce and order goods, the machines themselves, materials, methods and, importantly, the labour force.

The time horizon for this to really start is thought to be between 10 and 25 years from now. Not all the involved technologies have been developed to the operational stage. At present we are in a transition phase, which is the opportune time for re/insurance companies to become involved. Keeping up with developments and advising clients now can help to ensure their continuous engagement as Industry 4.0 is implemented.

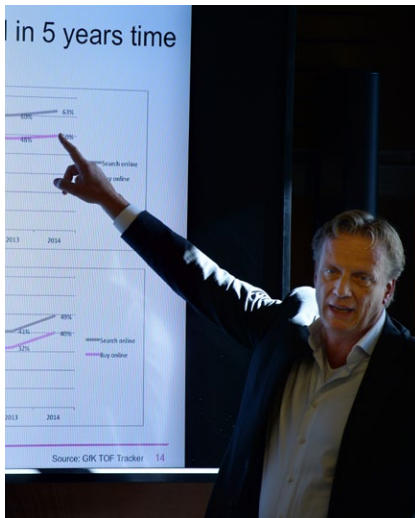
The risk management implications of smart manufacturing are:

- Difficulties in determining liability for losses as machines take over from humans
- Driverless vehicles
- Increased vulnerability to cyber attacks
- The challenge of data-flow security
- Business interruption
- Value chain disruption
- Changing labour requirements

A major Industry 4.0 challenge that will face insurers is the stacking and accumulation of risks attributable to the extreme interconnectivity and interdependence along the entire value chain. For modelling, this means that previously uncorrelated risks become correlated. For insurers to remain relevant in this imminent future, they will have to place more emphasis on their role as problem solvers, service providers and insight providers. They will need to have a sufficiently deep understanding of the developments to distinguish themselves from other strategic consultants.



## 2. 100% digital insurance



*Felix Tenniglo, Managing Partner, InShared*

In the Netherlands, traditional insurance sales channels have been disappearing rapidly for a couple of years. In 2014, 50% of non-life sales and 40% of life sales were online, and these figures are growing. Launched in 2009, InShared is a 100% digital insurer offering a broad range of non-life products with life products in development. InShared is based on the unique proposition that of the total premiums collected, 80% is allocated to claims, and the remaining 20% goes to cover costs. If less than the 80% is needed to meet claims, the remaining sum is given back to the customers as a cash refund. InShared has the highest NPS score in the Dutch market, far above that of the traditional insurers, and it has the lowest cost ratio. InShared takes care of its 250 000 customers and 500 000 policies with a staff of 36 FTEs. This is possible because the company automated whatever could be automated and what could not be automated has been sourced in or out.

A few years ago, InShared visited Google who mentioned that the initial focus had been on mobile devices before deciding whether to include PCs. Their claim was 'Mobile first'. When InShared recently spoke to Google again, the claim was changed to 'Mobile only'. InShared adopted this philosophy as well, which resulted in an even better and simple site and process. The big challenge in devising the selling systems for mobile devices was not the technical IT aspect, but the fact that you need to show sufficient information on a rather small screen.

Traditional insurance companies started developing their IT systems in the 80s and 90s, creating multiple product systems, more than one customer database, and several claims systems, all of them connected. InShared refers to that as a spaghetti of IT systems and connections. And it is this spaghetti that hinders traditional insurers from entering the digital age and being truly ready for online insurance sales.

Being a greenfield, InShared started from scratch in creating one integrated administration. It means one single product system, one claims system and one client system. They ensured that customers could read everything easily whatever the size of their display. InShared also took care to make their texts readily understandable, and they provide a fast and extensive FAQ package personalised in a virtual agent, who deals with about 90–95% of customers' questions. Overall, InShared provides customers with maximum self-service, and the model is highly successful.

To buy InShared car insurance, for example, customers only have to answer 6 questions, and by doing so, the company's system gathers the additional information needed (from databases for fraud, payment behaviour, licence plates etc). In 5 to 10 seconds, the client knows whether he is accepted and what the price will be.

### 3. Cyber risk management



*Nicholas Kitching, Head Governmental Affairs EMEA, Swiss Re*

The CRO Forum working group on cyber risk has been looking at ways to help improve cyber resilience and support understanding of the factors that can contribute to the accumulation of risk arising from writing cyber insurance.

Data is the new currency and insurers are targets for cyber attacks due to the sensitive data they hold on their customers. For organisations, the three main threats from cyber attacks are data breach, compromised availability of service and loss of data integrity. All these are likely to incur some form of financial loss, either through reputational damage, theft of intellectual property, regulatory fines or business interruption.

In developing a framework to support cyber resilience, the working group has identified four basic tenets building off best practices:

- Prepare: understand your data assets, your capabilities to address different levels of risk and establish a risk appetite
- Protect: undertake threat and control assessments, due diligence and incident response plans
- Detect: develop continuous monitoring and detection capabilities
- Improve: support continuous learning from events


These principles and other ideas are set out in a paper published by the CRO Forum, which describes steps that CROs can take to promote an awareness culture and build up cyber resilience in their organisations. Communication is a key component in this, particularly breaking down technical jargon into readily understandable terms, so that all members of a company can take risk-mitigating action. As organisations move up the technology scale, they develop different vulnerabilities. However, people will always be a key vulnerability.

The case of the hack on Sony in 2014, which resulted in a multitude of different and significant losses, holds valuable lessons. It highlights the need to be aware of the wider context and to notice clues that an attack may be imminent. These include factors such as threats that could indicate that a company is a target, internal organisational tensions and potentially historic diplomatic relations between countries. Risk officers need to be alert to these issues to respond on a timely basis and mitigate risk.

Insurance can play a key role to promote cyber resilience and mitigate the impact of a cyber event. However, the challenge for the provision of cyber risk insurance is around understanding of the price given the lack of data around the cost/impact from cyber risk. The CRO Forum is currently looking at a methodology for capturing cyber risk data that can support quantification of the impact of cyber risks both for the purposes of promoting efficient investment in cyber resilience and enabling effective scenario analysis for underwriting purposes.

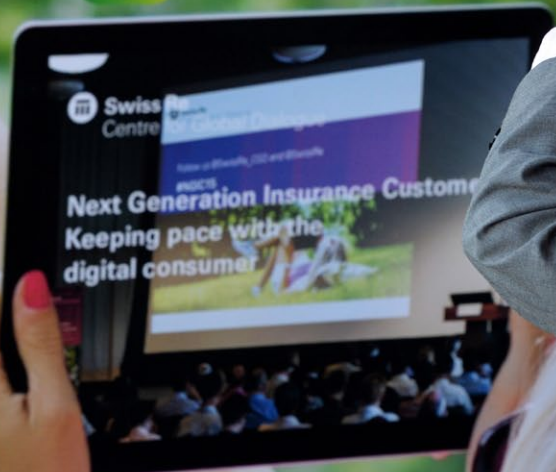




 **Swiss Re**  
Centre for Global Dialogue

## New conference report app

Download free to your tablet from App Store or Google Play



## Session 2: Big data and the data protection challenge

### Autonomous driving cars and big data: how to maintain trust

*Simon Hania, Chief Privacy Officer, TomTom*

Enormous sums are being invested in the development of autonomous cars, and their introduction is just a matter of time. The American approach, embodied by Google, is to go straight for the endgame of a totally driverless vehicle, while the European, mainly German, car manufacturers favour a phased introduction with gradually rising levels of autonomy. Whatever the approach, the robocars represent a paradigm shift at least as big as the transition from horse buggies to motor vehicles. To be viable, the new cars will need mapping and positioning systems with an unprecedented level of accuracy. They will also have to be aware of the road and weather conditions and they will have to know about hazards beyond the immediate horizon of their sensors. Furthermore, driving in these vehicles must be comfortable and should not cause travel sickness.

Using robocars will involve the generation and processing of very large amounts of data. Even if this is anonymised, it will trigger data protection issues, especially concerning location privacy and in particular for Europe, whose data protection laws are much stricter than those of the USA. Several years ago, TomTom was embroiled in a serious controversy, triggered by the fact that the police in the Netherlands used TomTom data, obtained through an intermediary company, to determine where to place speed traps. The press reported this fact but in some cases in distorted form, alleging that the use of TomTom navigation devices increased the risk of being fined for speeding. It was unfair and inaccurate, but resulted in a breach of trust situation because people felt that the data they had provided had been used against them. The company changed its contracts to prevent the use of its data for speed enforcement, and it realised that it had to request the permission of device owners before using their data, even when data is anonymised.

You have to explain to people  
why you want their data to reduce  
paranoia and build trust.

*Simon Hania, Chief Privacy Officer, TomTom*





A key learning for TomTom was that if it pulls data from a device in a car that is not strictly necessary for the services provided to the driver, it has to request consent. Data-gathering organisations must explain to people what the data is used for and they must reassure customers that sharing their data will not put them at a disadvantage. Otherwise, it could result in paranoia, which can very rapidly spread. European data protection laws in their current form would be problematic for the introduction of autonomous cars in Europe. Since regulations are currently being revised, however, the problems may not arise.

## Data privacy

*Eric Hilgendorf, Professor of Law; Chairman of the Department of Criminal Law, Criminal Justice, Legal Theory, Information and Computer Science Law, Julius-Maximilians-Universität Würzburg*

The subject of data privacy has attracted increased attention since Snowden's revelations. In October, the European Court of Justice ruled that US data protection standards were flawed and inadequate, drawing harsh responses from the US. Some Europeans, too, are sceptical about their own data protection laws, regarding them as obstacles to business innovation, to combatting crime, and the free flow of ideas and information. On the other hand, since Snowden's revelations, there is a growing concern even in the US over data protection, and the European model is gaining support. Large US companies like Microsoft already begin to comply with European standards of data protection, at least for their European customers.

Many of the ideas on privacy that are now highly influential in Europe originated in the USA. However, the two regions parted ways on data protection in the 1970s. The US war on drugs and later on terrorism involved the collection of large amounts of data. The relevant laws were reinforced after the 9/11 attacks, and the Patriot Act was passed. A wide variety of private data is still being recorded and processed by the US intelligence services, especially on foreigners. Big US corporations also hold much data on US citizens, and some companies have handed data to the security services. For a long time, this approach has been regarded as robust in the US. Personal data finding its way into the public domain in the USA can be accessed, stored and used, with restrictions only for business secrecy and preventing unlawful discrimination.

The development of privacy in Europe has been influenced by the 20th century experience of totalitarianism. Germany's Nazi regime consolidated its power in large part through an efficient system of gathering information on its citizens. Similar considerations apply to the Soviet Union under Stalin. The Gestapo, KGB and East-German STASI would have been even more powerful and repressive if they had greater access to data. In Europe today, data may be collected by the State or other entity only when specifically permitted by law or with the consent of the individuals concerned. Two basic principles are minimisation (only the minimum amount of data needed for the purpose may be gathered) and purpose limitation (data may be used only for the purposes for which it is collected).

# Recent European history largely explains European sensitivities regarding data protection.

*Eric Hilgendorf, Professor of Law; Chairman of the Department of Criminal Law, Criminal Justice, Legal Theory, Information and Computer Science Law, Julius-Maximilians-Universität Würzburg*





So the US and European approaches to privacy have been fundamentally different, at least during the last 40 years. Since that technology is largely US-driven, the American take on data protection has been gaining ground outside the USA. As a result, Snowden's revelations are now considered relevant for the whole world. Europeans actively post data on themselves, some of it problematic from a legal point of view, on social network platforms. Many young Europeans did not attach great importance to the question of data privacy. This, too, seems to be changing. As the imminence of smart homes and the Internet of Things brings the potential for even greater surveillance, the law must be adapted. Nowadays, a compromise between the US and the European models seems to be likely. A problem for the Europeans is that their relevant laws are now partly out of date. The US data protection law seems to be in an even worse state. On the other hand, Alan Westin's famous book on "Freedom and Privacy" (1967) and the landmark German Census Case judgement (1983) can be applied to today's digital technology with only minor changes.

Breakout sessions

Enhancing and protecting data usage in insurance

1. CRO Forum: Risk management and Big Data

*Fredi Lienhardt, Big Data & Smart Analytics Centre Manager, Swiss Re  
Stefano Nanni, R&D and Open Innovation Executive, Unipol*



A CRO Forum Working Group has drafted a paper on Risk management and Big Data that the Forum will publish in January 2016. The implications of Big Data and Analytics for the insurance industry and risk managers have been discussed and tested with an expert audience prior to publication.

Data has always been insurers’ raw material, but Big Data will affect the insurance landscape, leading to new opportunities as well as risks. Big Data is more than a buzzword; it involves:

- **Insights:** In a measured world, risks get more transparent and concepts such as predictive maintenance, self-driving cars are becoming real, leading to a potential transformation of existing risk pools due to the resulting change in severity and frequency of claims.
- **Hyperconnectivity:** People, machines and objects are becoming more and more connected. This can lead to increased interdependencies and more complex value or supply chain networks. The insurance industry needs to understand what it means for accumulation control as well as existing business interruption solutions.
- **Ownership:** There is a clear trend of moving away from actually buying assets (eg car, music etc) to services (eg Uber, Spotify). In addition, we will see a change in risk ownership and potentially an impact on insurance products.
- **New risks:** New technologies such as digitisation and cognitive computing bring new risks. The question arises, what risks will come after cyber risk? Insurers need to carefully monitor new and emerging risks, which, due to the rapid pace of the digital world, might emerge quickly.
- **Engagement:** This refers to digital distribution, collaboration and engagement with the policyholder. What are the needs of tomorrow’s insurance customer? How will insurance be bought or sold? Can we transform insurance into a positive experience?



Insurers now have more information on risk, the market and policyholders, but will have to decide which business models to adopt. They will also need to evaluate opportunities from a compliance and ethical perspective in a changing regulatory environment.

The entire insurance value chain will be impacted. Internally, the digitisation of business processes will lead to evolutionary changes, improving what insurers have always been doing. Risk monitoring, portfolio steering, fraud detection and reserving will benefit as the volume of data increases.

Externally, digital distribution, mobility and changing customer needs will lead to new business models and new insurance products. With digital native companies such as Apple and Google exploiting the close relationship with their customers, some insurers have started to explore new innovative insurance solutions. For instance, policies can be offered via apps to make purchasing easier. Companies that already hold data on individuals can leverage this data to help them fill in complicated forms when buying insurance products. Engagement systems that allow insurers to stay in close contact with customers may lead to the development of innovative insurance related services that potentially result in loss prevention, more customised products and increased brand awareness.

These business opportunities are relevant for the CRO function. CROs, however, should pay special attention to three areas:

- Governance/Compliance: In a dynamic and difficult to predict regulatory environment as well as a political environment where public opinion can be very influential, reputational and business risks need to be monitored.
- Partnerships: In a world of Big Data, partnerships with universities, vendors and other business partnerships become an important success factor. Insurers will need to deal with organisations that have a different risk culture and risk appetite.
- Risk culture: In order to formulate accurate second opinions on pricing, underwriting and claims management processes, CROs will have to define risk management needs in terms of skill sets, technical tools, risk and organisation culture.

## 2. Use of data in predictive underwriting and healthcare claims management

*Stephen Bishop, Head of Corporate Underwriting (Health), Munich Re*



Underwriting is a key component of risk assessment and the correct pricing of risk. Medical underwriting has come under political pressure and has actually been “outlawed” under the US Obamacare health reform. The result for the insurers there has been worse loss experiences. Under such constraints, predictive underwriting can be a business differentiator and improve competitiveness in saturated markets. It involves the use of internal or external data to achieve an improved underwriting selection or pricing for renewal or new business. External data improves the predictive capability. Although predictive underwriting can eliminate solidarity within insurance pools, it is actually used to determine who should pay what price. The underwriter can then introduce an appropriate degree of solidarity. The larger the data set provided, the more efficient predictive underwriting is.

Predictive underwriting can use existing data to build statistical models to forecast individual claims. Alternatively, it can use data to build scoring models for expected healthcare costs. It takes into consideration factors such as lifestyle, age, education, profession, marital status and where individuals live, among other factors. The scoring model can be as effective as sophisticated medical underwriting. Thirdly, existing claims history can be used to predict future claims and format up-sell/cross-sell campaigns for products with minimal underwriting requirements.

With regard to model use in practice, business analytics improves the effectiveness of CRM throughout a customer’s life cycle. A thorough understanding of how to use models is essential for those employing them, eg tele-sales teams. Models should be regularly tested and validated, and predictive underwriting drivers should be checked and validated with the business.

A significant number of claims can be auto-adjudicated with predictive techniques. Companies can decide between deterministic rules-based systems or probabilistic likelihood models or a combination. Claims adjudicators will probably be freed up to concentrate on the most complex claims.

CROs can encourage use of predictive techniques to improve return on marketing and acquisition costs, minimise mis-selling by targeting the right customers, improve fraud detection and develop new products. The main risks of employing predictive methods are:

- Potential consumer group protests about solidarity principles
- Reproach that poorer life and health risks may be penalised and denied access to insurance
- Models may identify sensitive social issues such as:
  - Age
  - Regional locations
  - Professions
  - Income levels

### 3. Natcat modelling in an open source framework



*Beat Aeberhardt, Head NatCat Tools, Swiss Re*

*Dickie Whitaker, Chief Executive, Oasis Loss Modelling Framework*

Oasis is a flexible NatCat loss modelling framework allowing the application of plug-and-play NatCat model components. It is based on open-source software technology and is available for free to all Oasis members, its non-profit status being protected by the fact that it is owned by a group of about 45 insurers and reinsurers. Oasis allows hazard, vulnerability and other interface specialists to offer their products via an e-commerce store, and it gives users the choice of provider, method of integration and IT environment. It provides full uncertainty information and enables users to choose their view of risk. Although Oasis is an open-source tool, the models developed for the framework will generally not be; Oasis does not own the models or model components and has no direct legal connection with the producers. However, Oasis defines some guidance to model developers to ensure the models available fulfill the high standards Cat models have to fulfill. The advantage of open source is that it creates a sustainable, very cost-effective environment with resilient architecture (because savvy users are always willing to upgrade it). Oasis is a convenient combination of open source with commercial components.



Swiss Re's NatCat group considers Oasis to be an extremely practical framework, because it allows easy integration of external components into our internal platform and sharing of models developed by Swiss Re outside the company. Because it is an independent framework, Swiss Re could use it jointly with a client to develop a model without the constraints of closed-source rating platforms, like issues arising if one of the companies changes to another model vendor. Oasis is able to open the NatCat modelling marketplace to more players and foster the creation of more models. It will facilitate a move away from the monolithic view of NatCat modelling dominated by a few players to a more diverse view of risk resulting in better understanding.

In addition to commercial use, Oasis has broader societal applications. Developing countries are encouraged to enhance their understanding of risk, but one of the challenges they face in this regard is a lack of knowledge and experience in building and using models. The high cost of commercially available vendor models is also a factor. To address this, they can download the Oasis software free, utilise the vast amount of online training offered, then start collecting useful data and understand how to build appropriate models. Data and models are at the heart of the current convergence of developing countries' needs and the interests of the insurance industry.



#### 4. Expanding organisational boundaries and new ways of managing data risk



*Raj Singh, Group CRO, Standard Life*

For many companies, organisational borders are changing as activities are increasingly outsourced to third-party providers. A further factor is the deployment of mobile workforces accessing company data while travelling or at home, sometimes via personal devices. This is occurring in a complex, constantly changing regulatory environment. So while new ways of working provide business benefits, it is becoming increasingly difficult to understand where data is and confirm its security. The impacts of inadequate data management are apparent from recent cyber attacks like the much publicised theft of personal information of 80 million clients of US health insurer Anthem.

Although employees are the main source of data compromise, the number of incidents attributable to business partners is growing. This is problematic because organisations' security considerations usually apply to their own perimeters rather than those of third-parties. The regulatory challenge is a further complicating factor: as data flows across global boundaries, how can the source organisation keep up with constantly evolving regulation and legislation, especially in the absence of consistently agreed and adopted standards? The problem is exemplified by the recent European Court of Justice declaration that the Safe Harbor data-transfer agreement between the EU and the USA is invalid. The Court deems American data protection law to be inadequate.

The data risk landscape is changing for several reasons, including increasingly complex supply chains, rising use of "niche" suppliers (whose security might have gaps), increased data flow outside the organisation's borders, growing use of the Internet, and other factors. These call for innovative risk management approaches underpinned by comprehensive employee awareness programmes. The cost of security, in terms of internal assurance over the control environment and external assurance over third parties, should not be underestimated, and the issue of where to set the spending threshold has to be considered.

While we can exploit the opportunities offered by technology, we have to understand the associated risk and the level of risk we are willing to take. Organisations have to ask themselves whether they understand the data they hold, its criticality to operations and whether the security applied to it is commensurate with its importance. Are business continuity plans keeping pace with external links and third-party providers, and could the organisation continue to function in the event of a large-scale outage?



## Panel discussion

### Industry perspective on the data challenge



*Moderator: Anke D'Angelo, Chief Compliance Officer, Swiss Re*

#### Panellists

*Eric Hilgendorf, Professor of Law; Chairman of the Department of Criminal Law, Criminal Justice, Legal Theory, Information and Computer Science Law, Julius-Maximilians-Universität Würzburg*  
*Bernhard Kaufmann, Group CRO, Munich Re*  
*John Scott, CRO, Zurich Global Corporate, Zurich Financial Services*  
*Andrea Splitt-Fischer, CRO EMEA & Asia, Swiss Re Corporate Solutions*

Insurance is a trust-based industry that has handled lots of client information for decades. But now digitalisation and the vast amounts of data available have created a new dimension and greatly increased need for security, especially for the more sensitive information like healthcare data. So far the insurance industry has not been the primary target of hackers, but the cyber attack on Anthem shows there is no room for complacency. Appropriate levels of risk mitigation must be applied without taking defence so far that the efficiency of the systems is hampered. Above all, the customers must trust the insurers with their data, knowing it will not be misused.

About 70% of insurers now work with big data, and as the amount of data increases, the challenge is to analyse it efficiently and use it appropriately rather than drown in it. The companies who are making effective use of big data and also using the new technologies to gain access to vast numbers of people are Google, Apple, Facebook and Amazon (GAFA). These were not even Fortune 500 companies 15 years ago, but are now the organisations who can really be said to “own” their customers. Taking GAFA as an example, the insurance companies that will profit most from digital technology are those who gain direct access to the customers, give them readily understandable information and turn a necessary, hitherto boring, purchase into something quick and easy. To achieve this customer-friendly speed-to-market, the insurers will need greater agility and openness to new ideas, like 24/7 pricing or claims handling. The tools at present will be the smartphone, tablet and desktop. The traditional distribution channels (like the agent route) are probably going to vanish. A major challenge will be to balance speed and agility with the traditional role of insurers as long-term stewards of capital.

Insurers have so far given little attention to the customer experience and a sense of community, which are the strong points of GAFA. So the insurance sector has a disadvantage by comparison with those high-tech organisations, and it will take time to catch up. For that reason, it may be sensible for insurers to attempt to team up with the new companies in some way, at least during a transition period.











## Session 3: Changing societies and evolving risk landscapes

### Assessing the risk landscape in the energy sector

*Christoph Frei, Secretary General, World Energy Council*

There is a sense of uncertainty in the energy sector, attributable to issues of speed and complexity. Up to 2008, shale gas had hardly been a topic of discussion, but only five years later, it had transformed the energy profile of the USA, turning it from an energy importer into an exporter. Gas prices collapsed and import terminals were converted into export terminals. Other recent changes include a drop in solar prices, plummeting oil prices, movement in electricity storage costs, and the abrupt change in the nuclear outlook following Fukushima. The speed of transformation of the energy landscape has been accompanied by increasing complexity with regard to price signals and investment factors.

The energy leaders' chief worries at present are price volatility, economic uncertainty, market design and electric storage. The topics they are currently working most intensely on are regional interconnection, renewables, energy efficiency and transitioning subsidy regimes. Apart from national subsidies intended to improve energy affordability for the less well-off, the main schemes have focussed on support for action taken to move away from fossil fuels and subsidies on renewables. The mindset has changed dramatically over the past year, however, and now goes in the direction of applying caps at the outset and having subsidy exit strategies.

The major risk preoccupations of the energy sector are extreme weather, cyber threats, the climate framework and the energy-water nexus. Cyber concerns are high in network industries like the utilities and in the OECD countries, due to their intense interconnectedness. Many governments seem to underestimate this issue. There are regional differences in attitudes to extreme weather risk: it is a major preoccupation of the Americas and Asia, but much less for Europe. Extreme weather is low on the agenda of oil and gas and taken more seriously by the utilities. The leap in the frequency of extreme weather events over the past five years has been accompanied by an international trend away from "hard resilience" towards "soft resilience". Realising that building to resist extreme weather will not always be successful, the alternative strategy is to accept that there will be damage and build in a way to allow rapid reconstruction. The movement is from impact-resistant, hard systems (fail-safe) to soft (safe-fail) systems. A further element of soft-resilience thinking, influenced by the experience of Hurricane Sandy, is that critical components have to be autonomous or locally controlled in order to prevent wider-scale breakdown and ensure black start capabilities. The energy-water nexus risk is subject to greater regional differences than weather risk, and is a major concern in Latin America, MENA (Middle East and North Africa), Africa and China.

# Speed and complexity together define the uncertainty in the energy sector.

*Christoph Frei, Secretary General, World Energy Council*



Three popular energy-related forecasts are that demand growth will be met by clean energy sources; global CO<sub>2</sub> emissions can be reduced by 50% by 2050, and universal electricity access will be achieved in the next 15 years. Unfortunately, these views turn out to be eminently debunkable myths – unless we dramatically accelerate innovation, adapt business models and implement a clear and effective CO<sub>2</sub> price scheme.

## Digital health

*James Heywood, Co-Founder and Chairman, PatientsLikeMe*

Mobility is a critical aspect of health, and a simple test involving how fast people can stand up from a sitting position on the floor is a good predictor of survival. Yet essentially no health system in the world tracks mobility information. This is an example of how the health industry chooses not to collect very inexpensive data that could make a difference. In addition, even when we do measure disease outcomes, the data we use to assess health varies with every disease, so that we cannot make comparisons and it is difficult to do integrative, holistic research or care.

Digital health is the consumerisation of molecular diagnostics and instruments to measure health and then delivery of actionable (sometimes non-actionable) medical information to the patient directly, bypassing the medical system. The huge and growing PatientsLikeMe database yields valuable information on symptoms and the efficacy of specific treatments. It can be consulted not only in terms of gender and age, but also for far more refined sets of parameters. A user could ask, for example, what treatments for depression or insomnia have been effective in 45 year-old females with multiple sclerosis. Cancer-sufferers could look up what experimental drug cocktails have been employed in their particular form of the disease and with what outcomes. For mental health, the information in the database rivals the data from all the clinical trials combined in terms of its holistic ability to explain and manage the disease. This is in contrast to clinical trials, which yield data that is precise, but measured in contexts that have increasingly less relevance to real-world, heterogeneous populations. Big digital health data is weaker at answering individual causal questions, but due to its quantity and breadth of measurement, it can be astoundingly useful. The emerging digital health system involves consumer health and behaviour monitoring (for instance with trackers such as Fitbits) and the use of consumer medical devices. This is changing the frequency and quality of the information we receive about ourselves, providing a view of people in the real world.

The way digital health works challenges the traditional model and it will severely disrupt the current economics.

*James Heywood, Co-Founder and Chairman, PatientsLikeMe*





The prediction is that the new, digital approach to health will gain ground and legitimacy slowly during an initial period as the technology evolves. As its utility starts to emerge and be validated, it will very rapidly be adopted. When that occurs, it will dramatically improve our ability to predict health with a high degree of accuracy and with time frames of weeks, months and years. It will change the way we diagnose disease. Treatments will be holistic and driven by big data. It will transform health care, severely disrupting the economics of the current model. Overall, this increased predictability will reduce uncertainty and therefore the opportunity for risk management by the insurance industry. At the same time, it will increase the ability of the system to improve outcomes. There is a danger that it will initially increase inequality and amplify social stress, because in its early phase, value will largely be available to the wealthy. Ultimately, it should improve all lives for the better.

## Breakout sessions

### Emerging societal risks

#### 1. The impact of political and regulatory developments on insurers

*Sean McGovern, CRO and General Counsel, Lloyd's*



Post financial crisis, the politics of regulation have strongly impacted the financial services sector and the insurance industry. This constitutes a present and emerging risk that is easy to diagnose but hard to mitigate. For the last five years, Lloyd's has regularly identified regulatory change and instability as one of the biggest risks it faces. Before the financial crisis, much of the emphasis was on principles-based, light-touch supervision and the notion that markets could be relied on to regulate themselves. Post-crisis, that is now considered completely wrong, and a massive new regulatory infrastructure has been built up with new macro-prudential institutions and refocused macro-prudential supervisors with strong mandates. Although the financial crisis originated in the banks rather than in the insurance industry, the insurers are seen as belonging to the financial services sector and are confronted with this new reality. This new reality operates at the global and regional levels as well within each country, and represents a present and emerging risk.

One factor that has made the environment even tougher for insurers is the fact that the changes are more politically driven than in the past. While regulation used to be drafted by specialists in consultation with the industry, much of the agenda is now driven by politicians whose watchword is "the tougher the better." One of the main reasons for this is that even after the financial crisis, the financial services industry, certainly in London, has been at the origin of a series of scandals, and the politicians demand a vigorous regulatory response to each new emerging issue.

The multiplicity of responses to the crisis around the world has challenged the notion of convergence and consistency. We are faced with an increase in localisation of capital and activity but the development of global standards. These seem to be pulling in opposite directions. Further consequences could be excessive and inappropriate capital standards and increased corporate governance standards. An example of the latter is the UK's Senior Insurance Managers regime, which rectifies the failure hitherto to hold any individuals accountable for the financial crisis.

A consequence of this is that CROs and compliance officers have to be able to reassure board members that the different regulatory regimes are being tracked as they develop, and appropriate risk management and compliance systems are in place. It involves being able to scan the horizon and interpret the implications so the Board is properly informed and strategic decisions can be made.

## 2. Credit risk



*Thomas C. Wilson, CRO, Allianz SE*

Credit risk is integral to the insurance business model: it is the by-product of long-dated assets that are used to manage a firm's asset/liability mismatch position. It is also a by-product of reinsurance transactions used to manage peak exposures and capital. Credit spreads or risk and liquidity premia, the flip-side of the risk/return coin, are also a significant driver of shareholder and policyholder earnings. In taking on credit risk as long-term investors, insurers also support economic development and capital formation in the broader economy. Changing regulation, monetary policy and financial markets are influencing insurers' credit decisions and society in wide-reaching ways.

Ten years ago, a risk-free or low-risk investment strategy for insurers entailed obtaining duration through government bonds and yield through real assets, offering guarantees of around 80% of the government rate and gaining upside for the policy and shareholders with the rest. This business model has been turned on its head in the low interest rate environment. In addition, because of the sovereign debt crisis in Europe, the strategy can no longer be regarded as low risk.

Various forces are affecting the credit decisions of insurers. These include regulatory changes, especially Basel III, the European Capital Markets Union and Solvency II. Macro-economic policy developments are also exerting an influence, especially quantitative easing leading to low rates and volatile markets, and the removal of tax incentives for retirement saving. These factors are in interplay against a demographic background of ageing populations.

### 3. Political risk in High Growth Markets: perspectives for the insurance industry



Nina Arquint, Head, Qualitative Risk Management, Swiss Re  
Beat Habegger, Head Political Risk, Swiss Re

For an insurance or reinsurance company, political risk can be defined as the probability that a particular political action or decision will change the economic and financial situation of companies and investors. Since political risks hold out the possibility of events that can entail loss or gain, they present both threats and opportunities. Underwriting can be directly affected since political dynamics shape the economic growth and development of a market, and adverse political events can negatively impact insured property, payments and people. At the operational level, politically motivated violence can threaten an insurer's own property, personnel and systems, and political dynamics can also affect the value of the company's investments. Politically influenced regulation or sanctions could have a very harmful effect on business opportunities. Considering the wider context, McKinsey, in its June 2015 global survey, rates geopolitical instability as the strongest threat to both domestic and global growth.

Four key political issues relevant to Swiss Re at present are:

- Global power shifts, which offer increasing insurance penetration and investment opportunities in emerging markets, but are accompanied by socio-political, regulatory and environmental volatility.
- The sovereign debt crisis and the future of the European Union. This issue raises questions about the viability of the monetary union, protectionism, low investment yields due to low interest rates, and the problems of migration and the refugee influx.
- Political violence producing regional turmoil with global knock-on effects. Examples are Syria, Iraq and radical Islamism, Russia and Ukraine.
- Terrorism risks with potentially severe negative impacts on the global economy. For insurers, this requires specific modelling and risk management capabilities.



Swiss Re's approach to political risk is based on continuous monitoring of events worldwide. Different scenarios may be drawn up and studied together with other risk specialists, like the financial risk management team. Reputational risk is always a consideration. Specific risk investigations entail sharp focus on the relevant geographical area and market, the lines of business and strategy. When all the elements of information have been collected, they are entered into an analytical framework and a tailored political risk assessment is produced. On that basis, the company can draw up risk mitigation measures. These can entail proposals for action to avoid potential losses or to seize opportunities. Decisions on these possibilities would usually be taken at the executive level.



#### 4. CRO Forum: Casualty accumulation risk

*Eric Schuh, Head Casualty Centre, Swiss Re*



Casualty accumulation risk is the concentration of insured risks or insurance coverages that may be affected by events or circumstances which cause substantial losses under several insurance policies, and potentially over multiple years and geographies. Well known examples of claims complexities based on casualty accumulation centre on asbestos, the Mont Blanc tunnel accident and the Deepwater Horizon incident.

The challenges faced by the re/insurance industry in terms of detecting and managing accumulation potential in the casualty portfolio are rendered more formidable by the interconnectivity and interdependency of the world due to globalisation, digital technological advances, regulatory changes and macro-economic factors. Complex and interdependent supply chains spanning countries and companies can magnify minor issues. The fast-evolving digital technologies provide unprecedented access to information and globalise problems. Regulation enhances transparency on potential risks of products, and new forms of litigation ease access to the courts while increasing the prospect of mega-awards. Thus the risk of casualty accumulation increases and must be managed. Portfolio steering provides an approach to managing the in-force risk and ensuring positioning for the future. This entails gaining a clear understanding of the in-force exposure and its potential for casualty accumulation scenarios, defining liability portfolios in line with risk appetite for those scenarios, and taking action to steer the portfolios towards the targets.

As a tangible example, there is a growing number of casualty claims stemming from property claims: examples being the California wildfires of 2007 and the 2009 Victoria brush fire. The key drivers of the trend are the rising frequency and severity of catastrophic events, diminishing acceptance of the "act-of-God" concept, greater transparency brought by the media, and an increased scrutiny by shareholders, analysts and auditors. Swiss Re approaches the issue of accumulation via forward-looking modelling based on Swiss Re Liability Risk drivers (LRDs). The LRDs are periodically assessed; perceived changes in the risk landscape can be immediately factored in, and external and group-wide data are combined to calibrate the model. Scenarios provide transparency on loss drivers and allow the accumulation risk to be managed. Exposure data of high quality and forward-looking casualty event sets are key for assessing the casualty accumulation exposure and weakening a potential threat to the balance sheet. Increased transparency of exposure enables further risks to be underwritten.

For more background information on casualty accumulation risk, refer to the CRO Forum working paper on the topic at:  
<http://www.thecroforum.org/casualty-accumulation-risk/>



## 5. Smart cities, smart living



*Silke Heuser, Senior Project Manager, KfW Development Bank*

The number and intensity of natural disasters have been rising in recent decades with a corresponding increase in disaster-related damage. Only about 30% of the damage is insured in developed countries and the figure is much lower in developing countries. Apart from the more frequent and intense hazard events attributable to climate change, the drivers of the increasing damage are population growth in areas at risk, with the consequent increase in built up infrastructure in those areas.

KfW Development Bank is working out methods and investment programmes to help developing countries cope with the damage caused by natural catastrophes. A recent example is provided by KfW's partnership with Swiss Re and consulting companies to study future risks for the cities of Barisal in Bangladesh and San Salvador in El Salvador, using Economics of Climate Adaptation (ECA) methodology. For Barisal, Swiss Re's CLIMADA program was employed to estimate the costs and benefits of different adaptation measures with a 30- and 50-year time horizon. Since the investigation considered only infrastructure, the outcome was adjusted by means of a multi-criteria analysis. The resulting information was intended to help decision-makers in the city authorities and in the German development organisation to prioritise climate-adaptation activities with a view to reducing the risks in the most cost-efficient way, and with the help of a 30 million EUR investment programme for the city. A post-study survey yielded mixed feedback, but KfW will continue with monitoring activities to see what measures are effectively taken up and implemented.

Included in the adaptation measures is a component of weather-based index insurance. It is in the insurers' interests to help to lower climate-related risks and to increase their presence in developing countries, which may be important future markets. But KfW has found that insurance projects like the one proposed for Barisal are not always taken up. Examples of successful schemes are a risk pool among small Caribbean states and the African Risk Capacity (ARC) insurance. The latter is taken out by governments but payouts go directly to the people affected. The scheme has a sanction mechanism to ensure that funds are appropriately distributed in the event of claims. ARC was backed up with USD 55 million reinsurance underwriting from twelve companies, including Swiss Re and Munich Re.







### The future of work in the sharing economy

*Arun Sundararajan, Professor, New York University, Stern School of Business*

A new generation of service-providing platforms based on non-debt, pure-equity financing is emerging. The ten biggest platforms - based in the USA, China, India and Europe - are already starting to rival incumbent firms in their industries in terms of market capitalisation. These platforms have created communities connecting providers of goods and services to consumers. The highly varied offer includes short-term accommodation (AirBnB), point-to-point transport (Uber) and labour. The system has been made possible by the population-scale adoption of technologies that facilitate the digitising of social capital. Despite the “sharing economy” designation, the scheme is solidly market-based, though there is a notion of “gift economy” in the transactions, an element of connecting and community. Visibility on social media and through the apps seems to create more robust forms of trust. Last summer there were days when a million people were staying at AirBnB properties. By comparison, the world’s biggest hotel chain has 700,000 rooms on its books. Uber is now valued at the level of a middle-sized car manufacturer.

Transport occupies a major part of the new economic scheme: four of the top five funded platforms are transport-based, and two of those are in China (Didi Kuaidi) and India (Ola). The Chinese market will soon be three times bigger than the US market. The new middle class in China and India is hundreds of millions strong, and many of its members can afford a car for the first time. Didi Kuaidi and Ola are trying to convince them to leapfrog the car ownership phase and buy transport on demand. The two companies see robocars coming and want to be the interface through which their customers access these. Part of their thinking is that demand will flow to the companies whose digital platforms the consumers trust rather than to brands associated with vehicle ownership. This dovetails with the thinking of the firms developing robocars: they are not targeting the taxi industry, they are targeting the car industry.

The new sharing economy companies might not replace traditional firms in every industry, but they will become an ever larger fraction of our economic activity.

*Arun Sundararajan, Professor, New York University, Stern School of Business*



There is a significant dimension of regulatory risk associated with these platforms in all sectors. At the heart of the concern is the blurring of lines between personal and professional. The regulatory systems, set up for conventional companies and individual professionals, are struggling to accommodate the new “casual” providers. The value of the new companies in the near term will be driven by how rapidly the regulatory systems adapt.

Current research suggests that as we move further towards an economy of services on demand, the transition will be good for the economy overall. The issue of taxation regarding casual working has to be tackled and measures are being taken. A particularly knotty problem is the funding of the social safety net. In the USA and the UK especially, this is largely tied to conventional full-time employment, so new partnership models have to be established.



## Ageing, demographics and societal change

*Walter Kielholz, Chairman of the Board, Swiss Re*

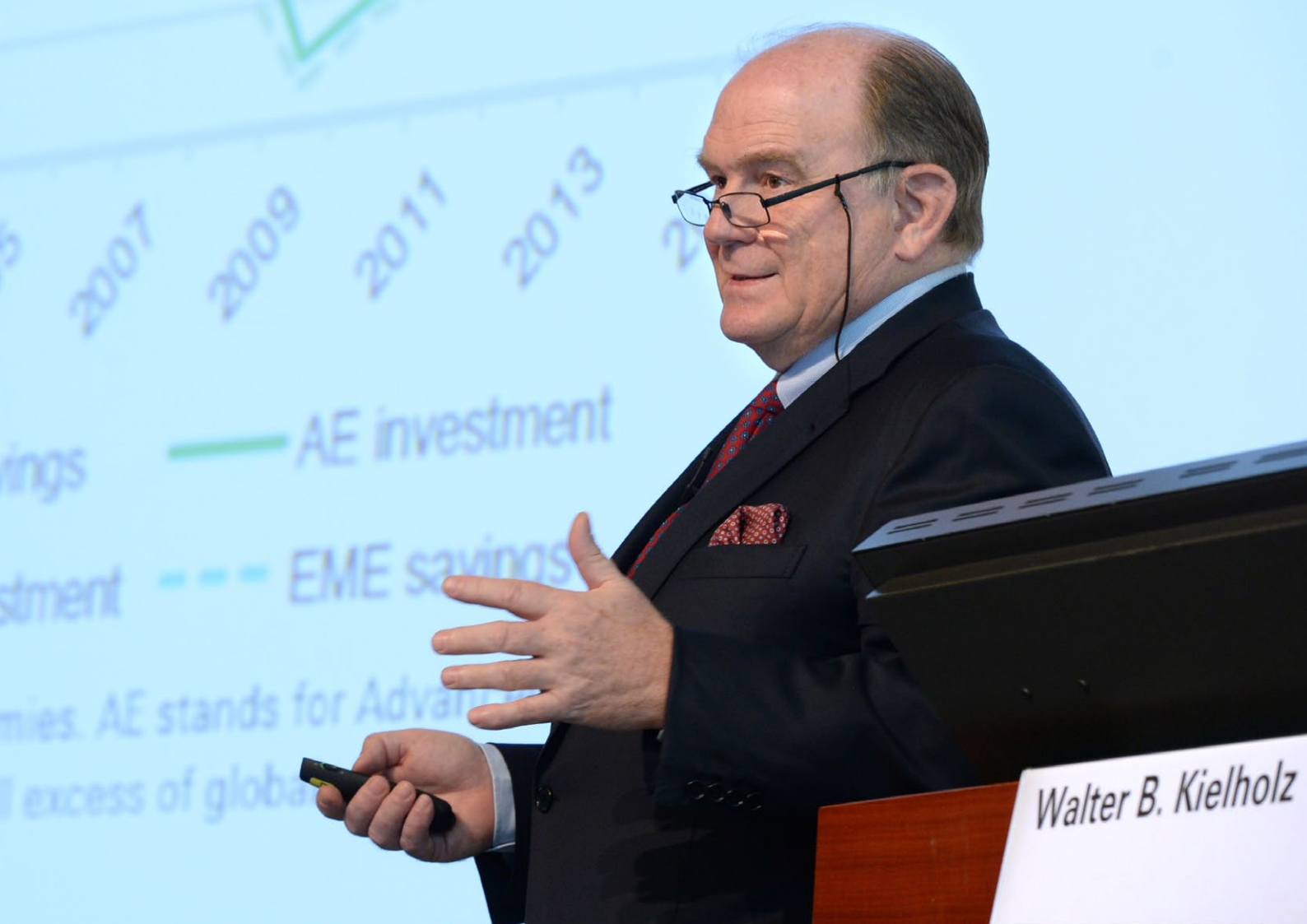
In many countries, the proportion of elderly people in the population is growing rapidly while overall population growth is slowing. Ageing and shrinking populations are especially prevalent in Europe and in China, due to its one-child policy. By 2050, of the advanced markets only the US will have working age population growth above zero. Among the major emerging markets, only India will.

The developed nations accumulated their current wealth before their populations started to age. In the emerging markets, however, the risk is that populations will age before their nations become wealthy, and this will have serious political and societal ramifications. In some countries, immigration can mitigate the effects of a shrinking workforce, but it also can be a politically sensitive topic. For example, in Switzerland the proportion of immigrants per capita is already very large. An influx of EU immigrants in the latter part of the 2000s, mostly highly educated specialists, added to the high number of foreigners, and there was a national vote on immigration in 2014. A slender majority of the Swiss population voted in favour of curtailing immigration. Anti-immigration sentiment is spreading in other European countries also, and immigration remains an important political issue in the US too. There has never been much immigration to Japan and it is therefore not a solution to the “silver tsunami”. For China, there would simply not be enough immigrants to make up the shortfall in the working population. Of course, not every country can bolster their population through immigration at the same time. Therefore, other means for increasing the workforce are necessary. These include increasing the proportion of female employees and raising the retirement age. However, the latter can be difficult politically, and requires a change of mindset with respect to expectations of entitlements.

What are the repercussions of these developments on the insurance industry? The Swiss Re Economic Research & Consulting “S-Curve” shows that in high-income countries such as the US, Switzerland and Canada, insurance penetration is high. In middle-income countries, insurance premiums rise faster than GDP, as is the case in China with its growing urban middle class. However, if incomes do not rise overall because of a shrinking workforce, insurance penetration slows and can even decline. In the advanced markets, the appetite for investment is diminishing and fixed capital formation as a percentage of GDP has been going down for years. China has had a long phase of building up fixed capital, but apart from China and India, there is no growth in this parameter either. Gross fixed capital formation is a major driver of property insurance, and influences other insurance lines. However, given the

# There is no short-term way of rectifying adverse demographic developments.

*Walter Kielholz, Chairman of the Board, Swiss Re*



property insurance protection gap, there is still potential for premiums to grow, particularly in emerging markets. However, it will need a continuous increase in productivity and fixed investment, as well as an expansion of the workforce, to end the negative growth dynamics.

The life insurance industry is more exposed to ageing and demographic changes. The advanced economies need to invest savings effectively to generate sufficient returns, which are not available in the current low interest rate environment. Investments can be made in emerging markets, where returns are higher, while also helping to fund and accelerate their growth. However, for Swiss Re's initiative to invest in infrastructure in emerging markets to work, there needs to be a supra-national agreement to protect the firm's investments.

Life insurance is a possible solution to the lack of savings and low returns. Premiums in the emerging markets are rising much more rapidly than in the advanced economies. In particular, there is strong growth in life insurance savings products in Asia. In western economies, the declining attractiveness of life insurance and a great reluctance to buy long-term care products presents a real challenge for the industry. Nevertheless, health and long-term care are areas where insurance can contribute to longevity and well-being, while generating premium growth.

Ultimately, however, the reaction of societies to demographic challenges is political. Societies have become much more conservative in Europe in the last few years. Ageing populations will form the political majority in the near future and are shifting policies towards their needs, conserving the achievements of the last decades, while resisting technological advances. However, by doing so, they risk destroying some of their societal gains of the past several decades.

The CRO Assembly is an annual conference for information-sharing among CROs outside The Geneva Association and the CRO Forum.

The CRO Assemblies are organised by The Geneva Association and the CRO Forum in collaboration with major insurance and reinsurance companies – this year together with Swiss Re. The goal of the annually hosted events is to promote understanding of modern risk management in insurance and the role of the CRO. This is done through a series of workshops and studies and other initiatives in this area.

They allow attendees to share their experiences and to get to know colleagues with similar responsibilities in other insurance companies and also create a forum in which to deal constructively with strategic issues facing the insurance industry through direct contact with a global network of leading experts.

Another objective of the CRO Assembly is to spread and discuss risk management knowledge with other sectors and help cross-fertilise ideas and concepts.

## Organisers

### **Swiss Re** Centre for Global Dialogue

The Swiss Re Centre for Global Dialogue is a platform for the exploration of key global issues and trends from a risk transfer and financial services perspective.

Founded by Swiss Re, one of the world's largest and most diversified reinsurers, in 2000, this state-of-the-art conference facility positions Swiss Re as a global leader at the forefront of industry thinking, innovation and worldwide risk research.

The Centre facilitates dialogue between Swiss Re, its clients and others from the areas of business, science, academia, and politics.



Founded in 1973 by the CEOs of global insurers, The Geneva Association is an international insurance think tank that produces and distributes high-quality research and analysis on global strategic insurance and risk management issues.

Our research promotes policy-related and public discussions among our Members, academics, standard setters, policymakers, governments, international organisations and the public at large. Our objective is to educate and develop understanding on the unique role and importance of insurance in economies and for societies through publications, conferences and active discourse with policymakers and others.

The Association takes an active role in discussions with policymakers, central bankers, regulators and supervisors on behalf of the insurance industry.



The CRO Forum is a group of professional risk managers from the insurance industry that focuses on developing and promoting industry best practices in risk management. The Forum consists of Chief Risk Officers from large multinational insurance companies. It aims to represent the members' views on key risk management topics, including emerging risks.





© 2016 Swiss Re. All rights reserved.

Publisher:  
Swiss Re Centre for Global Dialogue

Author:  
Jeffrey Barnes

Editor:  
Brian Rogers

Photography:  
David Ausserhofer

Design:  
Corporate Real Estate&Logistics/  
Media Production, Zurich

The entire content of this publication is subject to copyright with all rights reserved. The information may be used for private or internal purposes, provided that any copyright or other proprietary notices are not removed. Electronic reuse of the data published in this publication is prohibited.

Reproduction in whole or in part or use for any public purpose is permitted only with the prior written approval of Swiss Re Centre for Global Dialogue. Courtesy copies are appreciated.

This publication is for information purposes only. It does not constitute any recommendation, advice, solicitation, offer or commitment to effect any transaction or to conclude any legal act of any kind whatsoever. Any views or opinions expressed in this publication are solely those of the author and do not necessarily represent those of Swiss Re. Anyone shall at its own risk interpret and employ this publication without relying on it in isolation. Although all the information used in this report was taken from reliable sources, Swiss Re does not accept any responsibility for the accuracy or comprehensiveness of the information given or forward looking statements made. In no event will Swiss Re or one of its affiliates be liable for any loss or damages of any kind, including any direct, indirect or consequential damages, arising out of or in connection with the use of this publication and readers are cautioned not to place undue reliance on forward-looking statements. Swiss Re undertakes no obligation to publicly revise or update any forward-looking statements, whether as a result of new information, future events or otherwise.

Swiss Re Centre for Global Dialogue  
Gheistrasse 37  
8803 Rüschlikon  
Switzerland

Telephone +41 43 285 81 00  
[www.swissre.com](http://www.swissre.com)