WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Mitigating Risks in the Innovation Economy

How Emerging Technologies Are Changing the Risk Landscape

October 2017

World Economic Forum
91-93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland
Tel.: +41 (0)22 869 1212
Fax: +41 (0)22 786 2744
Email: contact@weforum.org
www.weforum.org

REF 260517

Project Team and Steering Committee

Project Team
World Economic Forum
Abel Lee, Head of Insurance and Asset Management Industries
Victoria Shirazi, Project Lead, Mitigating Risks in the Innovation Economy

Oliver Wyman (Adviser and Knowledge Partner)
Prashanth Gangu, Partner
Matthew Leonard, Partner
Laura McKay, Consultant

Contact
For feedback or questions, please contact:
Victoria Golshani Shirazi
Victoria.Shirazi@weforum.org

Sincere thanks go to our Partners for their valuable insights, thought leadership, contribution to this White Paper and overall support of the Mitigating Risks in the Innovation Economy initiative.

Contents

Foreword

Consistent with the World Economic Forum's mission of applying a multistakeholder approach to address issues of global impact, the creation of this White Paper involved extensive outreach and dialogue with the insurance community, technology community, academia and government. The dialogue included numerous interviews and interactive sessions to discuss the insights and opportunities for collaborative action.

Sincere thanks are extended to the industry experts and emerging disruptors who contributed their insights to this White Paper. In particular, the members of the project's Steering Committee and Working Group played an invaluable role as experts and patient mentors.

Deep gratitude also goes to Oliver Wyman for its generous commitment and support in its capacity as the official professional services adviser to the World Economic Forum for this project.

Executive Summary

The core purpose of the insurance industry is to enable risk-taking, support economic growth, encourage innovation and enhance the resilience of society and the economy. Fundamentally, insurance allows individuals or entrepreneurs to manage risk better than they would without insurance.

In the past, when new risks emerged, the insurance industry was able to adapt and offer the necessary protection to society. However, the age of globalization combined with the digital era has led to unprecedented technological advances and breakthroughs globally. These developments will bring a radical shift in the nature of risks to society, and the insurance industry is expected to struggle to use its old playbook to address these emerging risks.

The growing interconnectedness in society will, in many ways, mitigate the risks with existing systems. However, accelerated digitization and growing open and connected digital environments are creating new vulnerabilities and potential consequences that are less predictable than ever before. The key challenge will be finding the balance between the risks and rewards of new technologies. As the world stands on the brink of the Fourth Industrial Revolution, the large benefits that these technologies bring must be embraced while preparing for a potential array of unforeseen implications.

Over the last year, the World Economic Forum project **Mitigating Risks in the Innovation Economy** has worked to examine how emerging technologies are causing a radical shift in the nature of risks faced by individuals, businesses and society. This information, gathered through research, interviews and roundtable discussions, was used to develop a shared set of recommendations among the Steering Committee and Working Group members to support society in anticipating and tackling the changes arising from the emergence of technological innovations.

In the future, the roles of insurers, governments, technology firms and risk owners will need to evolve to address the changing risk landscape:

Insurers

– Insurers need to play a larger role in risk education. As public and private organizations adopt new technologies, insurers will need to support them to better understand the risks of emerging technologies and ensure the appropriate risk management capabilities are in place to manage these new risks.

– The lack of historical data will require insurers to embrace alternative sources of information to better understand emerging technology risks. In addition to alternative data sources, insurers may consider new forms of modelling where past losses are not solely effective in predicting future threats.

– Predicting emerging risks is made difficult by general technical complexity and the lack of information regarding their potential damages. This could lead to large-scale adoption delays or higher prices. In the future, insurers should look to uncover and ultimately address protection gaps and unmet needs. At times this may require harnessing digital innovation and advanced analytics to deliver new solutions.

Governments

– Some forward-thinking governments have navigated challenges related to emerging technologies by first establishing a framework upon which future governmental action will occur. By providing markets with their latest thinking on an emerging issue, governments are able to give markets a heads-up before introducing a new rule.

– Governments can accelerate the development and use of “regulatory sandboxes” to get ahead of the governance challenge.

Technology firms

– Technology players should start thinking of themselves not only as innovators, but also as stakeholders in shaping the future of risk mitigation. This industry has deep technological, data science and related expertise. As experts in this area, they have the opportunity and responsibility to take on a larger role in supporting the development of risk mitigation solutions.

Risk owners

– Consumers and companies will need to find ways to manage the trade-off between adopting innovations in an unrestricted way and taking the time to first understand their potential consequences. As already noted, the insurance industry may play an important advisory role in facilitating these discussions.

Despite the value in individual endeavours, emerging risks are shared by society, and there is little advantage in tackling the issues alone. Significant dialogue will be required between various parties – governments, insurers and technology players – to mitigate these new risks.

There are three areas in particular that should be prioritized

1. *Liability in practice*: Existing liability rules were not designed with complex and autonomous systems in mind, which has left stakeholders guessing as to how current liability rules will be applied in practice. Insurers, governments and technology players need to come together to accelerate the development of a solution to this large and pressing issue.

2. *Accessibility and usability of alternative sources of information*: The exchange of data can and will be an effective tool to support the management of vulnerabilities and threats. In the future, governments should continue to foster collaboration and the sharing of information between the public and private sectors. Insurers and technology players should take an active role in these initiatives.

3. *Harmonization of global protocols:* A patchwork of standards and regulations is likely to ensue if there is no collaboration across borders. The resulting risk is an environment in which new technologies must operate under an inconsistent set of safety and operational protocols globally. It is important to identify areas with significant gaps and promote the development of collaborative efforts to establish these global protocols.

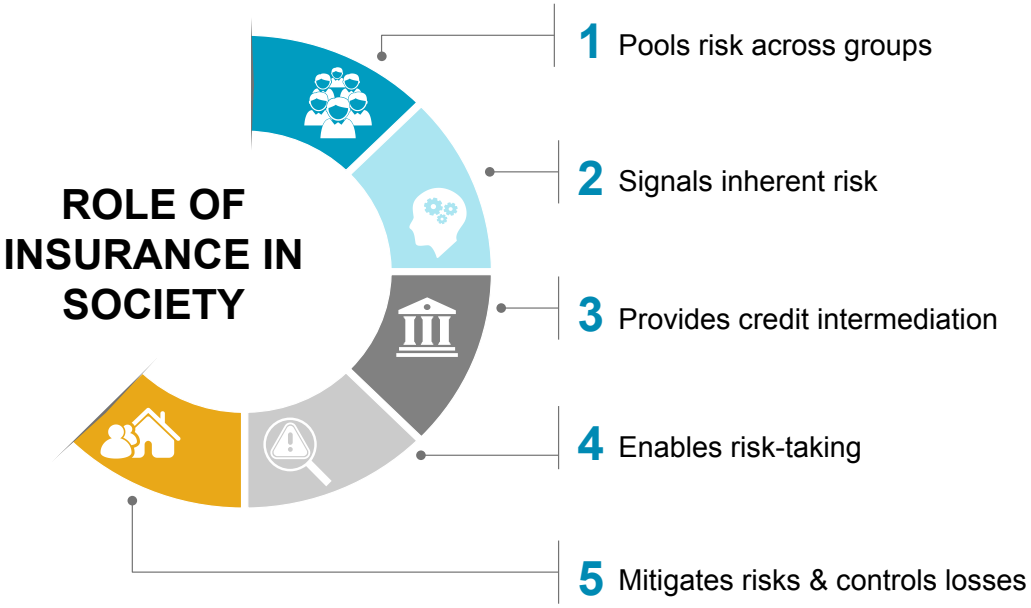
The World Economic Forum and Oliver Wyman hope this White Paper can stimulate further discussion and, where appropriate, prompt innovation among insurers, governments, businesses and technology players to help mitigate risk and improve resilience in society.

1. The Present Roles of Insurance in Society

Globally, insurance accounts for 8.8% of gross domestic product.[1] In some countries, that percentage can surpass 30%.[2] It would be hard to imagine a society without some form of risk protection. Despite the prominence of such economic activity, many are unaware of the various roles insurance and insurance institutions play in society (Figure 1). This section examines each of these roles to better understand how insurance fundamentally operates and how it is central to the functioning of society.

Figure 1: The Five Roles of Insurance in Society

Source: World Economic Forum and Oliver Wyman



1. Pools risk across groups

Insurance aggregates risks to provide more predictable outcomes.

As Winston Churchill put it in 1909, "Insurance brings in the magic of averages to the aid of the millions".[3]

In aggregate, risks are more predictable. The fundamentals of risk pooling involve measuring risks based on their statistical occurrence for a larger pool (and not for an individual). By pooling risks, the insurance industry spreads risk among a large number of policyholders. This aggregation decreases uncertainty and reduces the need for "precautionary savings"[4] (savings for unpredicted future losses) at the individual level, freeing up income to invest back into the economy.

Earliest forms of risk pooling

The concept of individuals forming bonds or groups with other individuals exposed to common risks is not new. Early risk instruments tended to be non-financial in nature (for example, splitting up cargo across a number of ships to avoid losing everything in the event of an accident).

Insurance instruments were not established until the 17th century. At that time, a growing number of merchants embarked on expeditions to the Americas and West Indies and faced the risk of losing their ships and cargo at sea. By insuring the risk, merchants could undertake these journeys without the fear of being quickly put out of business.

Around the late 1680s, sailors and underwriters would meet at (Edward) Lloyd's Coffee House in London to finance these ventures, each writing their name and the amount of risk they were insuring on a piece of paper.[5] Soon, Lloyd's Coffee House gained a reputation not only for providing "trustworthy shipping news", but also as a place to obtain the newly born marine insurance.[6]

2. Signals inherent risk

Insurance helps society make better decisions about risk.

By pooling and pricing risks, insurance allows individuals and businesses to effectively compare the cost of different choices.

How? From its origins, insurance has evolved in response to society's need to better understand risks. Early on, maritime insurance underwriters relied on qualitative information, such as the type of vessel, reputation of the crew and the route taken.[7]

Since then, the insurance industry has progressed in its ability to measure and identify risk. Insurance is one factor that allows individuals to accept risks and/or pursue risk-mitigating alternatives. Policyholders often lack the expertise to understand why a safety precaution is justified.[8] Is it worthwhile to install fire sprinklers in a new building? Is it valuable to install an anti-theft device in a new car? The insurance industry quantifies the value of each of these risk-mitigating behaviours and generates price signals for the inherent risk of certain activities. This in turn allows individuals and businesses to effectively compare different choices.

3. Provides credit intermediation

The insurance industry reinvests capital in long-term assets.

On the investment side, the long-term nature of insurance liabilities and the predictable nature of premiums allow insurers to make long-term investments in many industries, such as agriculture, real estate and infrastructure. Insurers currently allocate approximately $2 Billion of their assets under management to infrastructure investments.[9]

As a result, the insurance industry serves an important function as an institutional investor in society and offers the "professional oversight" needed for these investments.[10]

4. Enables risk-taking

Insurance allows businesses to engage in value-creating activities.

Fundamentally, insurance allows individuals or entrepreneurs to undertake greater risk than they would in the absence of insurance.

Transport insurance helps manufacturers manage the risk of losing goods in shipment. Crop insurance protects farmers against the risk of drought and other unexpected losses.[11]

History offers numerous examples of the role insurance plays in promoting economic development. As discussed earlier, marine insurance played a tremendous role "in opening up European trade with the New World".[12]

The North Sea oil drilling industry is a more recent example. In the 1970s, oil drilling platforms were not only very expensive, but also exposed to risks "not previously experienced in the industry".[13] The insurance market and its "willingness to insure these new and costly technologies" played an important role in the development of the North Sea oil industry across Europe.[14]

"Historically, insurance has developed in close parallel with economic development and growth – and in particular with the development of manufacturing industry, as shown in the UK during the 19th century."[15] By freeing up individuals and businesses from common risks, insurance encourages innovation. As a result, "insurance has become a major economic sector in virtually every mature economy".[16]

The first insurance company

The first individual insurance policies did not emerge until the late 1600s. Their entrance in the market can be largely attributed to the Great Fire of London.[17]

At the time, hardly any of the 70,000 homes destroyed by the fire were insured.[18] The event would eventually trigger the creation of the first insurance company, The Insurance Office, in 1667.

The company was established to protect houses and commercial properties from damage caused by future fires, using fire insurance policies. The Insurance Office established firefighting teams to support this endeavour. The practice was simple: if individuals or businesses were insured, they were asked to place a plaque or "firemark" on their houses or buildings. The firefighting teams would then extinguish fires in buildings displaying these plaques.[19] This triggered the growth of the sector, and new insurance companies established their own product offerings and firefighting teams.

5. Mitigates risks and controls losses

Insurance incentivizes greater risk-reducing behaviour and protects society against otherwise devastating losses.

Insurers use loss and exposure information for another, more subtle purpose: to encourage risk mitigation. The same information that goes into pricing calculations is relevant in determining how to reduce risk.

Consider fire sprinkler systems, invented in the 1870s. Currently, fire sprinkler systems are critical to reducing the damage caused by fire incidents. When first invented, however, fire sprinkler systems did not get as much attention and praise as one would imagine. It was not until the insurance industry came to understand their benefits that sprinkler systems gained traction. How? Insurance pricing was used as a method of increasing the use of fire sprinkler systems and ultimately incentivizing better risk management practices.

A similar story can be told regarding the large-scale adoption of airbags. Automobile insurers were the first to petition for airbag regulations, which were adopted despite opposition from the automobile industry.[20]

All major insurance carriers offer risk management services to control losses. "[Insurers] analyse a policyholder's loss history, manage their prevention efforts, and teach them how to avoid premium increases."[21]

Why? At times it may seem counterintuitive, since the existence of risk prompts the need for insurance. But insurers promote risk-reducing behaviours for a few reasons. First, and likely most significant, is competition. By reducing the overall risk, insurers are able to offer discounted premiums that in turn help to attract more customers.[22] Second, insurers incentivize risk-resilient behaviour to attract "good risks" – for example, to select more profitable customers.[23]

The case of the US flood insurance market

According to the Insurance Information Institute, "Flooding is the most common and costly natural disaster in the United States, causing billions in economic losses each year".[24] However, following the Mississippi Flood of 1927, the possibility of "highly-correlated large losses" led the private insurance market to cease coverage.[25] This prompted the establishment of the National Flood Insurance Program (NFIP) to subsidize insurance payments for homes in flood-prone areas. This in turn led to what many believe is an act of "distorting subsidies to a harmful activity".[26] When a premium is priced in line with the overall risk, insurance can deter individuals from areas or activities of greater risk and can encourage the use of mitigation measures. On the other hand, if insurance coverage is heavily subsidized, it can weaken the policyholder's incentives to prevent and mitigate future damage. For example, elevating a home can significantly control losses in the event of a flood. However, if this is not reflected in a policy's pricing, policyholders may not have the incentive to invest in elevating their homes. By subsidizing premiums, the NFIP is encouraging riskier behaviours, including excessive development (and redevelopment) of disaster-prone areas.

The challenges of government-subsidized insurance programmes have been heavily researched. A recent study by Oliver Wyman provided a thorough review of reasonable options for privatizing the NFIP. According to the study, there are "several distinct reasons why increased private market participation in the flood insurance market would yield a more optimal long-term solution to managing flood risk … [including] innovation, market penetration and alignment of incentives and roles."[27]

So what?

Insurance remains an important enabler of considerable economic activity. Historically, when new risks emerged, the insurance industry was able to adapt and offer the necessary protection to society. However, as society progresses, the nature of the risks it faces is changing as well. Technological breakthroughs, such as the internet of things (IoT) and self-driving vehicles, are transforming society. New risks are emerging, and existing risks are becoming more complex. The insurance industry will struggle to use its old playbook to address these emerging risks.

The next section explores the changing risk landscape and the implications for the insurance industry and society at large.

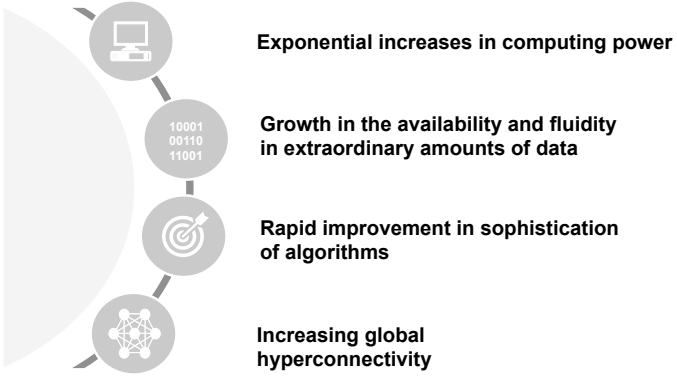
2. The Changing Risk Landscape

Powerful forces are driving a radical shift in the nature of risks facing society.

In the near future, inventions only seen in science fiction will be filling streets and homes (Figure 3). Artificial intelligence (AI) is already omnipresent – from personal assistants to drones to software that predicts people's music and movie preferences. Smart utilities are starting to come online in cities around the world. Most estimates have self-driving cars entering the market within the next decade, with many pilots already under way.

Figure 2: Powerful Forces Reshaping the Economic, Social, Cultural and Human Environment

Source: World Economic Forum and Oliver Wyman



The age of globalization combined with the digital era has brought about unprecedented technological advances and breakthroughs globally. A number of powerful forces are driving these changes (Figure 2), including the exponential increase in computing power, the growth in the availability and fluidity of extraordinary amounts of data, rapid improvements in the sophistication of algorithms, and increasing global hyperconnectivity.

When will the future arrive?

Figure 3: Tipping Points Expected to Occur by 2025

In March 2015, the World Economic Forum Global Agenda Council on the Future of Software and Society launched the Technological Tipping Points survey. Based on the council's discussions over previous months, the survey asked respondents for their views on 21 tipping points – moments when specific technological shifts hit mainstream society.

The survey results were analysed to see what percentage of the respondents expected the respective tipping points to occur by 2025, or 10 years from the date of the survey.

	%
10% of people wearing clothes connected to the internet	91.2
90% of people having unlimited and free (advertising-supported) storage	91.0
1 trillion sensors connected to the internet	89.2
The first robotic pharmacist in the US	86.5
10% of reading glasses connected to the internet	85.5
80% of people with a digital presence on the internet	84.4
The first 3D-printed car in production	84.1
The first government to replace its census with big-data sources	82.9
The first implantable mobile phone available commercially	81.7
5% of consumer products printed in 3D	81.1
90% of the population using smartphones	80.7
90% of the population with regular access to the internet	78.8
Driverless cars equalling 10% of all cars on US roads	78.2
The first transplant of a 3D-printed liver	76.4
30% of corporate audits performed by AI	75.4
Tax collected for the first time by a government via a blockchain	73.1
Over 50% of internet traffic to homes for appliances and devices	69.9
Globally more trips/journeys via car sharing than in private cars	67.2
The first city with more than 50,000 people and no traffic lights	63.7
10% of global gross domestic product stored on blockchain technology	57.9
The first AI machine on a corporate board of directors	45.2

Source: World Economic Forum, *Deep Shift: Technology Tipping Points and Societal Impact*, 2015

These developments will lead to a radical shift in the nature of risks to society. According to the World Economic Forum *Global Risks Report 2017*:

Production, mobility, communication, energy and other systems are changing with unprecedented speed and scope, disrupting everything from employment patterns to social relationships and geopolitical stability. Driven by the convergence between digital, biological and physical technologies, the Fourth Industrial Revolution is creating new global risks and exacerbating existing risks.[28]

In particular, two aspects of this revolution will be especially challenging. The first is speed. These new risks are unprecedented in how fast they develop and in the way they manifest or reveal themselves over time. The second is growing technological penetration. The past was characterized by the benefit of isolation. The internet of things, however, brings connectivity to devices that were previously isolated from each other, and the widespread digitization of everyday life will bring risks that penetrate every facet of society.

The following section explores these two elements and their effects on the existing risk-mitigating landscape.

2.1 Increasing clockspeed

"Clockspeed" was coined by Charles Fine in 1998 to describe the faster pace of life, in an industrial context. Through his research, he observed that the time from design to product launch is reducing, even for complex products.

In the last 30 years alone, the world has seen the rise of the personal computer, the internet revolution and the adoption of smartphones. Each development has felt more disruptive than the prior one. According to Ray Kurzweil, the American author, computer scientist and inventor, as new technology becomes more effective (e.g. as computer chips become more powerful while costing less), greater resources are deployed to further that progress. Currently, that means increased budgets for research and development, and recruiting top talent, all dedicated to further building and amplifying new developments.[29] The result is an accelerating rate of technological progress.

Kurzweil argues that the time lapse before the mass adoption of new technologies is shortening (Figure 4). In the 1800s, it would have taken over 30 years for a technology to reach mass adoption. Today, the speed of adopting innovations has drastically increased. In the 1990s, it took only seven years for the World Wide Web to reach mass adoption.[30]

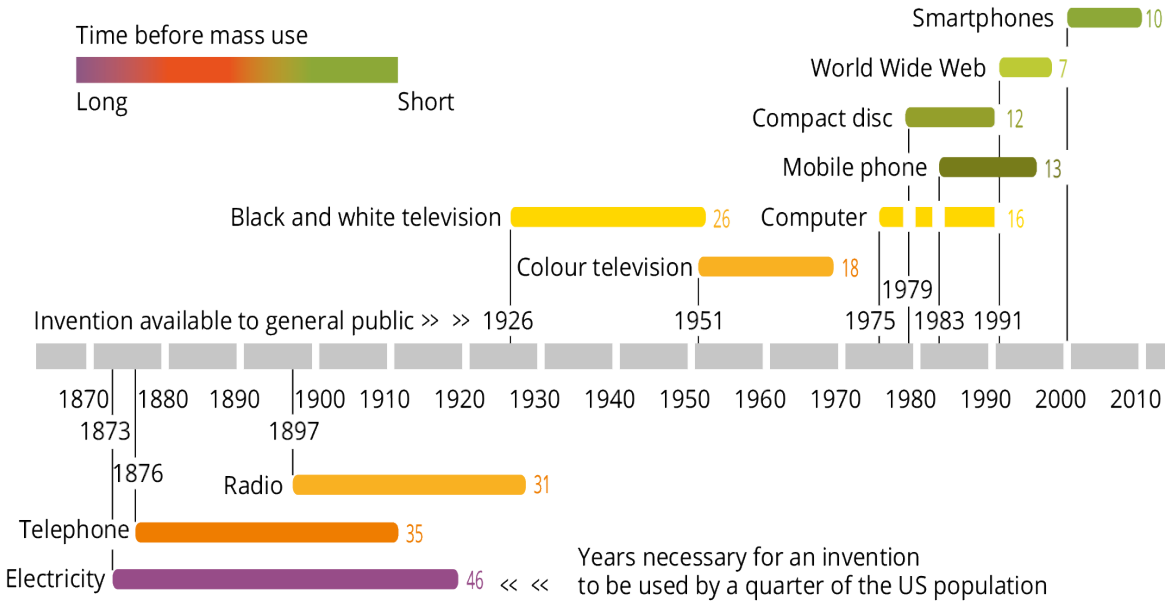
"We won't experience 100 years of progress in the 21st century – it will be more like 20,000 years of progress (at today's rate)." [31]

Ray Kurzweil, Founder and Chief Executive Officer, Kurzweil Technologies, USA, in "The Law of Accelerating Returns"

Consider the rapid increase of computing power. Moore's law, which predicted that "the number of transistors (a computer's electrical switches used to represent 0s and 1s) that can fit on a silicon chip will double every two years as technology advances",[32] has held true even a half century after it was developed. This will continue to improve the ability to innovate and transform society at accelerating speeds.

Figure 4: Shortening Time Lapse before Mass Adoption of New Technologies

Source: European Environment Agency (EEA), *The European Environment – State and Outlook 2015: An Integrated Assessment of the European Environment*, 2015 (Figure 5.4)



All these concepts are contributing to important changes in the existing risk landscape. Risk decisions currently need to be made in a world with more complexity and uncertainty than ever before. The challenge is the availability of information to manage these risks.

Created in 2006, the term "risk clockspeed" defined "the rate at which the information necessary to understand and manage a risk becomes available".[33] Risks from select emerging technologies, such as AI and the IoT, fall into the category of "fast clockspeed risks", or those where insufficient time and information are available to understand and manage the new risk.

"It is hard to identify what harm a technology can cause until the technology actually causes that harm. In the past we have had the luxury of putting a lot of funding and research into predicting that harm. We don't have that luxury anymore – new technologies are emerging too quickly."

Andrew Maynard, Professor in the School for the Future of Innovation Society, Arizona State University

The pace of technological development and the paradigm shift for governments

The governance of emerging technologies is patchy: some are regulated heavily, and others hardly at all.
In the past, a new technology was usually developed in collaboration with the government or with government-funded entities (often for defence or military applications). Federal research and funding in the United States contributed substantially to the development of airframes and aircraft engines, a wide range of pharmaceuticals and biomedical devices, satellites, computers, biotechnology and nuclear power.[34] Governance and legal frameworks were considered alongside the development of these new technologies.

More and more innovation is being developed in the private sector, and at an accelerated pace. These innovations are being built and adopted on a large scale before governance tools are developed. Governments are struggling to understand how to use emerging technologies, let alone govern these advancements. For example, the US Federal Aviation Authority (FAA) took eight months to grant Amazon an "experimental airworthiness certificate" to test a particular model of drone, by which time the model was obsolete.[35]

The shift of public and private responsibilities is likely going to magnify challenges around risk control and mitigation in the future.

2.2 Growing technological penetration

"Technology already is controlling critical systems such as airline routes, electricity grids, financial markets, military weapons, commuter trains, street traffic lights and our lines of communications."[36] Intel predicts that up to 200 billion IoT devices will be in use by 2020, which equates to around 26 smart objects for every human being.[37] The widespread digitization of everyday life is creating a risk environment that is more unpredictable than ever before.

This growing hyperconnectivity is amplified by the development of cyberphysical systems. By removing the cyberphysical barriers, "we have been creating a risk environment that is greater than the sum of the risk of the parts".[38] In the past, the physical world had to ensure that a system malfunction or failure would not harm people or the environment, and was isolated from public networks. Therefore, it was less susceptible to cyberattacks over the internet. By combining the digital and physical worlds, the world's assets are facing unprecedented risks, leading to business disruption and critical infrastructure interruption, and even national security ramifications.

In February 2017, Amazon's S3 cloud storage system went down, causing large disruptions across the internet. It is hard to quantify the actual damages of such a failure, however. According to *The Wall Street Journal*, analytics firm Cyence has estimated that it cost Standard & Poor's (S&P) 500 companies at least $150 million.[39] Since the event, Amazon has acknowledged that "the root cause of the outage was an incorrect command executed by a staff member … during routine maintenance".[40]

"Cyber-risk is severe, and the insurance industry plays an important role helping companies identify risks and determine strategies for risk avoidance, mitigation and transfer."

Daniel Glaser, President and Chief Executive Officer, Marsh & McLennan Companies (MMC), USA; Member, Steering Committee

This example demonstrates how pervasive digitization and the growth of open and connected digital environments are creating new vulnerabilities and potential consequences that are less predictable than ever before. The interconnectedness will exacerbate existing risks (terrorism, geopolitical conflict) and may introduce a number of new risks (data privacy, cybersecurity).

However, painting these advancements as dangerous and malicious is not accurate. The growing interconnectedness in society will, in many ways, mitigate the risks with existing systems. Smart grid technologies, for example, are helping utilities "to speed outage restoration following major storm events, reduce the total number of affected customers, and improve overall service reliability."[41]

The key challenge of the future will be finding the balance between the risks and rewards of new technologies. As the world stands on the brink of the Fourth Industrial Revolution, the large benefits of these technologies must be embraced while preparing for a potential array of unforeseen implications.

Interconnected infrastructure challenges for insurers

The growing build-up of interconnectedness risk is creating challenges for the insurance industry. In July 2015, Lloyd's of London and the University of Cambridge Centre for Risk Studies, United Kingdom, published *Business Blackout*, a report that illustrated the problem facing the industry. The study demonstrated how a cyberattack against the US Northeast power grid could result in a multitude of seemingly uncorrelated claims.[42] The report reminds insurers that they could be faced with claims across many different lines of business, which emphasizes the need to further assess this growing build-up of interconnectedness risk.

In 2016, the Prudential Regulation Authority (PRA), the arm of the Bank of England overseeing the insurance industry, wrote a letter to chief executive officers (CEOs) of the insurance industry that highlighted interconnectedness risk build-up as a growing area of concern. One aspect of the letter focused on silent cyber-risk, where coverage is provided "inadvertently through a policy that was typically never designed for it".[43] The spread of silent risk across the market is highlighted as one of the key areas of concern by the PRA.[44] It states that this risk is "not only material, but is likely to increase over time and has the potential to cause losses across a wide range of classes".[45]

2.3 Technology roundup: New and changing risks of the innovation economy

Some risks have been assessed for years, including risks of mortality, natural catastrophes and sickness. Technological progress, on the other hand, is driving important changes in the existing risk landscape. New risks, such as data privacy and misuse of technology, were not top of mind 20 years ago.

A series of workshops in the fall of 2016 sought to identify those risks with the fastest clockspeed and the potential to pose the greatest societal impact. The aim was to get an early indication of the technologies requiring further discussion and attention.

Technological innovations were assessed across two dimensions:

1. **Clockspeed** – representative of the rate at which the information necessary to understand and manage the risks of this new technology becomes available[46]

2. **Societal impact** – broadly defined as the degree to which potential significant societal impact exists across a number of key risk categories, including:
   - Data security and privacy – Threat of privacy breach resulting in the ability to track people or technologies
   - Safety – Threat of physical injuries resulting from a product defect, user misuse, malicious act or lack of maintenance
   - Socio-economic – Threat to the future of employment, the viability of social security systems and the distribution of wealth and influence
   - Financial – Threat of severe economic losses
   - Operational – Threat of malfunction or failure of a technology or system on which society is highly dependent

Select findings of this exercise are highlighted in the following pages.

Unmanned aerial vehicles

Unmanned aerial vehicles (UAVs) have only scratched the surface of their potential. The emerging use cases of UAVs are growing, leading to ongoing change in society. Goldman Sachs Global Investment Research estimates the global commercial market opportunity for drones at $20 billion.[47] The largest market opportunity is in construction, followed by agriculture and insurance (Figure 5).

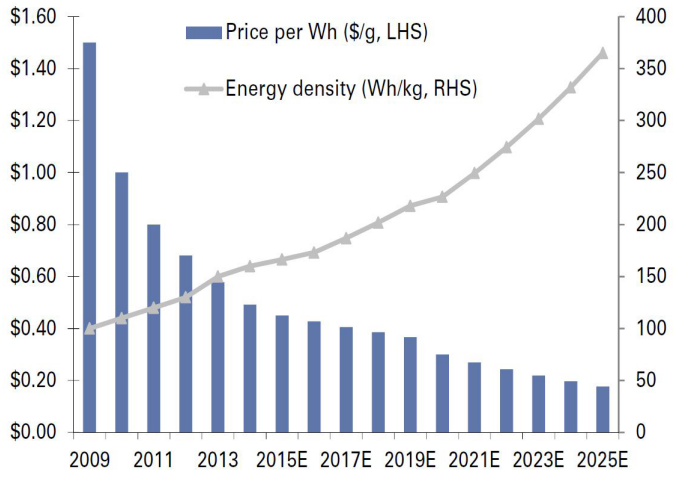
Figure 5: Global Opportunity of Drones Driven by Commercial Markets

Market	Total Addressable Market Globally ($ million)
Construction	11,164
Agriculture	5,922
Insurance claims	1,418
Offshore oil and gas, and Refining	1,110
Journalism	480

Source: Goldman Sachs Global Investment Research, *Drones: Flying into the Mainstream*, Profiles in Innovation, March 2016

Figure 6: Estimated Price of Automotive Lithium-ion Batteries and Density

Note: Wh = watt-hour; LHS = xxxx; RHS = xxxxx.
Source: Source: Goldman Sachs Global Investment



Most drones employ some form of lithium-ion technology, given they are small and lightweight. The batteries are well-suited for flights but have room to improve. Estimates show that these batteries will continue to increase in density (enabling longer, more efficient flights) and will decline in cost (Figure 6). This further demonstrates the growing opportunity for drones.

Drone delivery (not considered in these estimates) is the wild card and usually the most discussed application of UAVs. The size of the global parcel delivery market was estimated to be $300 billion in 2016.[48] Internet retail sales accounts for a large portion of this market, and sales in 2016 were up 25% from the previous year.[49] In fact, China has a growth rate of 35% per year.[50]

As the numbers indicate, the market opportunity for drone delivery is tremendous, significantly higher than other commercial markets. A number of companies have publicly discussed the potential for drones. Amazon Prime is leading these efforts, having launched a small private drone delivery pilot in the United Kingdom at the end of 2016.[51] Remarkably, Jeff Bezos, Chief Executive Officer, Amazon, tweeted in December 2016 that a package was delivered to a customer in Cambridge just 13 minutes after the order was placed.[52]

Key risks

Safety is the most critical threat when it comes to UAVs. The risk of a drone causing mass casualties by colliding with a commercial aircraft is central to this security threat, which became heightened when a drone came within 65 feet of striking a passenger jet as it flew above London's The

Shard skyscraper.[53] The UK government has commissioned a series of test crashes between drones and planes to find out exactly how much damage a drone could cause in a collision.[54] The research will be used to better inform regulators on this topic.[55] Additionally, a variety of anti-drone technology is currently in development and may reduce this risk, but its implementation and success is still too early to judge.

Currently, the impact of privacy invasion is limited, though the overlay of facial-recognition technology is potentially much more invasive.

Implications for the insurance industry

Patchy regulatory regimes and a lack of liability certainty continue to be issues in this market for insurers. The United States and the European Union are updating existing drone regulations to address some of these ongoing challenges. If solved, drones may provide a significant new underwriting opportunity.

A large demand for insurance on the consumer side, for applications such as recreation and photography, is unlikely unless a regulatory requirement is established. In the United States, the FAA lacks the authority to impose insurance requirements for UAVs (this will occur at the state or local regulatory level). Elsewhere, drone insurance is not required for consumer users, with a few exceptions, such as Italy.

Some demand for insurance exists on the commercial side. However, brokers have difficulty finding capacity for their commercial business. The aviation market covers damage to the drone itself, but not exposure to third-party liability or personal injury. The excess liability market is still in the early stages of covering this exposure.

Driverless cars

As an emerging risk topic, driverless cars are not new. In fact, the first self-sufficient and truly autonomous cars appeared in the 1980s, developed by the Navigation Laboratory (Navlab) of Carnegie Mellon University (USA).[56]

However, progress over the last three to five years has been outstanding. In the last year alone, the number of self-driving cars authorized to test in Silicon Valley has increased to 180, and the number of companies licensed has risen to 27 – "more than twice as many as a year ago and up from just seven in early 2015".[57] Furthermore, recent investments in the industry have been enormous. General Motors spent $1 billion to acquire Cruise Automation, a start-up in the self-driving vehicle segment, in 2016.[58] In August of last year, Uber reportedly spent $680 million on Otto, a self-driving truck start-up that was only eight months old.[59]

There is no doubt that the excitement for self-driving cars is building. Perhaps one of the best examples of this is the stock price for NVIDIA, which makes critical hardware for autonomous vehicles and whose stock price more than tripled between May 2016 and March 2017 (Figure 7).

Figure 7: NVIDIA Stock Price

Source: Google Finance

Is the technology ready for large-scale adoption? That is still open to interpretation, though reports in the past year point to a high level of sophistication across existing pilot projects. The California Department of Motor Vehicles (USA) recently released a set of "disengagement reports", which summarize the number of times people needed to intervene with the autonomous technology in pilots. The reports reveal important progress; Google's programme, Waymo, outpaced competition, logging only 124 interventions over 636,000 miles driven in 2016.[60] The company reported that most of those interventions were a result of discrepancies across the hardware and software, for example when "the car's lidar and camera reported slightly different data".[61]

Despite the hype, automotive experts generally predict a gradual shift from human drivers to autonomous cars.[62] Google, Ford and Uber have all said they plan to have fully autonomous cars in production by 2021, though it is not clear what exactly that entails. In a recent *MIT Technology Review* article, Steven Shladover, Research Engineer, University of California, Berkeley, predicted that these technologies will be very restricted: "Probably what Ford would do to meet their 2021 milestone is have something that provides low-speed taxi service limited to certain roads – and don't expect it to come in the rain."[63]

To enable widespread adoption, self-driving vehicles will need to confront a complex web of challenges, including significant regulatory and legal developments. To some extent, these will act as barriers to the speed of this technological development.

In the United States, the federal government offered a warm welcome to the industry when it released *The Federal Automated Vehicles Policy*, its guidelines for self-driving vehicles. However, the work is not done. A number of standards and laws that are incompatible with autonomous vehicle technology still remain.

Key risks

Safety was identified as one of the key threats of self-driving vehicles, particularly where a common platform is used by many. A cyberattack or disruption to a smart transportation system has the potential to result in mass injuries.
Two additional threats were identified that could pose significant societal impact. The first is an operational threat resulting from increased technical dependency on a smart transportation network. The second, more widely discussed threat is a socio-economic one, given the expected loss of transportation-related jobs (e.g. taxi drivers, truck drivers).[64]

Implications for the insurance industry

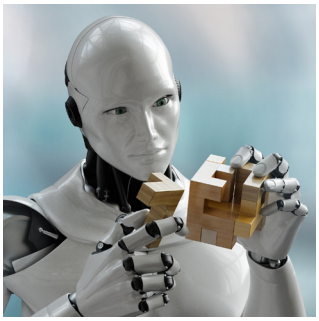
Driverless cars may be the most disruptive technology for the insurance industry in the last century. Automotive players are promising that their models will greatly improve safety on roads. If that is the case, the impact on the automobile industry will be tremendous. However, this is not a new concept: in 1998, Peter Lewis, Chief Executive Officer, Progressive, said, "The biggest risk we face is the end of auto insurance… at some time in the future there will be so many fewer, less severe auto accidents that it will disappear."[64]

Many reports are pointing to a slow progression to fully autonomous vehicles. In the near term, a gradual increase in safety features will lead to lower insurance premiums and more competition in the marketplace. As autonomous technology (e.g. autopilot features) gradually becomes standard equipment, insurers will better understand the impact on the frequency and cost of accidents.

The biggest challenge is likely to be the introduction of fully autonomous vehicles. In this case, many questions around liability remain. In general, experts believe this issue needs to be tackled under two dimensions: compensation (who pays for future damages) and safety (who is responsible for product safety).

This is a top priority for automotive insurers, and many are collaborating with the technology and automotive sectors to support concrete and narrow test cases, pilot programmes or demonstration projects. In 2013, Ford unveiled the automated Ford Fusion Hybrid research vehicle, developed in collaboration with the University of Michigan (USA) and State Farm. Further, Zurich Insurance Group is involved in several autonomous vehicle research programmes worldwide, including CitiMobil.

Going forward, the industry will need to collectively identify single forums to collaborate on legislative initiatives, standards developments and neutral discussions. At a company level, insurers will need to continue to invest in innovative modelling, simulation, data collection and analysis to better understand the risks posed by these new technologies.



Artificial intelligence

Artificial intelligence (AI) is already all around us, from personal assistants in homes to software that predicts people's music and movie preferences. Impressive progress has been made in AI in recent years, driven by exponential increases in computing power and by the availability of vast amounts of data.

In 2016, Google put numbers to its AI progress. The company's image recognition technology improved to 93.9% accuracy from 89.6% in 2014.[65] The technology now has the "capability to detect colours and analyse the content in images with more than one subject".[66]

Additionally, the company's natural language processing technology has moved beyond understanding short phrases to understanding more context. Google Translate was launched in 2006 and has since become one of Google's most popular assets. The translation system serves more than 500 million monthly users, translating 140 billion words per day into a different language.[67]

AI will be one of the top disruptions globally in the next decade. Bloomberg predicts that over the next few years, "all software applications could feature embedded AI" (early examples include Google Photos and Amazon Alexa).
The rationale is that as AI gains traction, competition will increase and regular apps will fail to survive against those powered by AI.[68]

Already, the successes of Amazon, Google and Facebook have demonstrated how "AI provides a competitive edge".[69] These case studies may heighten the urgency to adopt the technology, "as fears of being outflanked are sparked".[70]

Key risks

The most widely discussed threat of AI is the socio-economic one, including concerns about the future of employment, the viability of social security systems and the distribution of wealth and influence.

Financial and reputational threats may also be a top consideration for companies handing decision-making power to a machine. In March 2017, a number of large companies "pulled their YouTube spending after advertisements were found running alongside hateful and extremist videos".[71] According to an estimate by analysts

at Nomura Instinet, Google's parent, Alphabet, risks losing $750 million in revenue as a result.[72] To solve this issue, Google must "solve an AI problem no one has cracked yet: automatically understanding everything that's going on in videos, including gesticulations and other human nuances".[73]

Physical safety was also identified as a key threat of AI. One can only imagine the wide range of consequences resulting from a product defect, user misuse, malicious act or lack of maintenance.

Implications for the insurance industry

Where operator error is clearly identifiable, existing insurance models will continue to be sufficient. However, as these technologies become increasingly complex, it will be difficult to assess "what went wrong". Regulatory and legal uncertainty with robotics and autonomous systems is making risk assessment difficult, potentially leading to large-scale coverage gaps or higher insurance premiums.

The lack of liability certainty is one of the greatest issues in this area for insurers. How well do current products and policy wordings cover these new exposures? Do existing commercial policies include coverage for physical damage and business interruption caused by an autonomous system? How does a technology developer's liability policy or errors and omissions policy respond in the event of an autonomous system failure? These questions will need to be solved as AI continues to grow in complexity and scale.

Smart utilities and other smart infrastructure

Smart infrastructure is changing society. The Cambridge Centre for Smart Infrastructure and Construction estimates that such infrastructure is a global opportunity worth $2.5 trillion-6.0 trillion.[74]

What is smart infrastructure? The Centre defines this evolution as the "result of combining physical infrastructure with digital infrastructure, providing improved information to enable better decision making, faster and cheaper".[75]

Digitally enhanced or smart infrastructure is rapidly progressing across sectors. Smart grids, used to monitor and manage energy consumption in cities, are starting to come online globally. In aviation, advanced data-processing and communication technologies are digitizing the air traffic control system. Smart water technologies are optimizing the way water supply is controlled.[76]

Figure 8: Smart Metering – Implementation Sites, Projects in Demo or Deployment, 2002-2016

Source: European Commission, *Smart Grids Projects Outlook 2014*

To a large extent, the growth of these new innovations depends on the public sector's investment appetite. The European Union, for example, "aims to replace at least 80% of electricity meters with smart meters by 2020 wherever it is cost-effective to do so".[77] This ambition was set in 2014, and progress has been substantial (Figure 8). By 2020, according to the European Commission's 2014 report on smart metering, "it is expected that almost 72% of European consumers will have a smart meter for electricity. About 40% will have one for gas".[78]

Key risks

The largest threats identified were safety and operational. The increased risks of cyberattacks on vital city networks are still unclear, though energy, transportation and public services may become key targets of malicious actors.

Smart city innovations may also give rise to increased data privacy risks from the sharing, analysis and misuse of urban big data.

Implications for the insurance industry

Insurance companies are acutely aware that this growing interconnectivity within cities may lead to large loss accumulation.[79] In the case of a large infrastructure failure, insurers could be required to meet claims across many different classes of coverage, including direct damage, business interruption and third-party liability policies. The legal precedence regarding liability in a large infrastructure failure is mixed. The report *Business Blackout* examines this ambiguity in legal cases following the 2003 Northeast blackout in North America. In one case, Wakefern Food Corp vs Liberty Mutual, the court ruled that Liberty Mutual would pay service interruption claims to Wakefern for food spoilage that occurred in their supermarkets during the 2003 blackout.[80] However, in a number of separate cases, the court denied the requested service interruption payments.[81]

It is essential for the insurance industry to understand the increasingly complex and interconnected risk exposure and to develop strategies to manage that risk.

Smart cities can also trigger a demand for new insurance products, as these new cyberphysical infrastructure investments give risk to new vulnerabilities (technology interruptions, data privacy).

The internet of things

Cheap sensors connected to the internet are beginning to invade society.

On the consumer side, two of the trends discussed as part of the Mitigating Risks in the Innovation Economy initiative were wearables and smart homes.

According to International Data Corporation, the technology market analytics company, the wearables market has grown 3.1% year over year in the third quarter of 2016, with almost 23 million wearables being shipped every quarter.[83] Fitness bands accounted for 85% of the market.[84]

The smart home market, however, has failed to gain the same acceptance in the mass market. In North America, the number of smart home systems reached 16.9 million in 2015.[85] Only 2.8 million of these were multifunction or whole-home systems, with the rest accounting for point solutions.[86] This corresponds to a 9.7% household penetration rate in North America, the largest market globally.[87] The European market is still in its early stages, and two to three years behind the North American market in terms of penetration and maturity.

Technological fragmentation and issues around interoperability are making it difficult for consumers to set up and control multiple devices at once. This will continue to be a challenge for the smart home market until common standards are established.

Others believe the biggest challenge is technological – namely, "making the devices self-powering".[88] According to Juan Ignacio Vázquez, Professor of Telematics, University of Deusto, Spain, "while you can afford the inconvenience of having to recharge your phone more or less every day, it's too much of a burden to devote the same sort of daily attention to another five or 10 devices".[89]

Perhaps this is why many believe the industrial IoT (IIoT) market will be even more disruptive than the consumer market. GE believes the growth of the IIoT sector will be tremendous in the future: "[Consumer IoT estimates] are impressive numbers, but we believe they will be dwarfed by the industrial app economy that is now emerging. This is because industrial apps will leverage a massive installed base of physical assets across sectors that act as the engines of global economic growth: energy, healthcare, transportation."[90]

The total market for IIoT solutions in China grew by 82% between 2010 and 2015, equating to compound annual growth of 12.7%.[91] China has now become the largest market in key industrial automation categories, though IIoT growth rates can be seen globally.

The IoT market will continue to mature over the next five years, with a high rate of adoption.

Key risks

Connected devices can serve as new entry points for a privacy breach, and in some cases facilitate attacks on the network to which they are connected. In October 2016, a Chinese security-camera maker said its cameras were used to launch a cyberattack which left millions without access to a number of the world's most popular websites.[92] The attack has "underscored how hackers can marshal an increasing number of online gadgets to disrupt the internet on an unprecedented scale".[93]

Additionally, data privacy was also identified as a key threat of the IoT given the extraordinary availability of data provided by connected devices. These technologies will dramatically change the way personal data is collected, analysed and used in the future.

Implications for the insurance industry

Connected devices give insurers the opportunity to have more frequent and meaningful customer interactions. To date, the insurance industry has been slow to embrace digital models, which has sustained the low frequency of interaction between insurers and insureds. These new products allow insurers to connect with their customers in innovative ways. State Farm, for example, offers a discount on homeowner policies for installing a Canary home security monitor.[94] Similarly, American Family Insurance offers its home, condominium and renters policyholders a 5% policy savings when they purchase the Ring Doorbell (which allows answering the door using a smartphone).[95]

A home data feed could help insurers notify clients of much-needed maintenance or repairs before they cause major damage.[96] The data from these feeds, however, is difficult to incorporate into legacy underwriting systems. Insurers have not been using these data feeds in the pricing of homeowner's policies on a large scale, aside from providing customer acquisition discounts.

Connected devices may also trigger the opportunity for more tailored insurance solutions for both manufacturers and operators of smart devices to protect against security and privacy risks.

The sharing economy

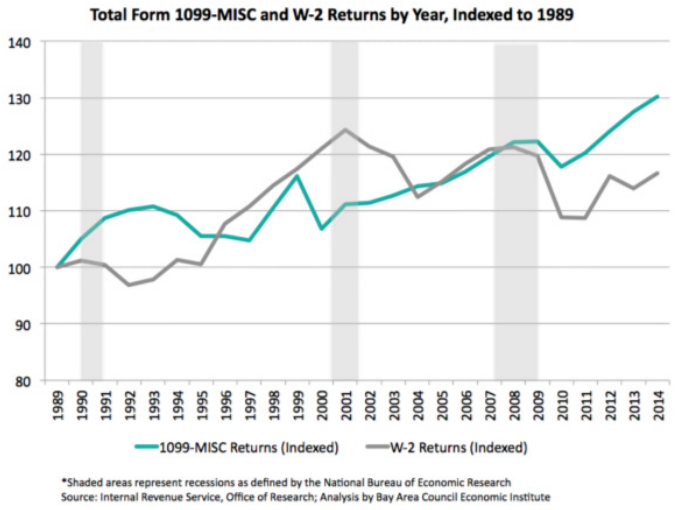
The sharing economy, otherwise referred to as the gig economy or the on-demand economy, is a form of collaborative consumption built on a foundation of technology.[97] These platforms were built on "recognizing and minimizing economic inefficiencies" – for example, an excess of privately owned cars but a lack of parking spaces.[98]

Globally, the sharing economy includes 17 companies worth more than $1 billion, with 60,000 employees and $15 billion in funding.[99] Uber's market value was recently reported at $60 billion, or higher than 80% of all S&P 500 companies.[100] The sharing economy is undoubtedly growing at an accelerating pace.

This growth has significantly impacted the workforce worldwide. In the United States, the number of contract workers, sometimes referred to as 1099 workers ("1099" refers to the Internal Revenue Service form 1099-MISC used by independent contractors), is increasing.[101] In the past, a growth in 1099 workers was common after a recession. Figure 9 reflects the growth of these workers after the 1990, 2001 and 2007-2009 recessions. However, since the end of 2009, or the last recession in the United States, the growth has steadily continued.[102] Many believe this is due to the growing number of sharing economy platforms that "have made participating in the 1099 economy much easier".[103]

Figure 9: Total Form 1099-MISC and W-2 Returns (US), 1989-2014, Indexed to 1989

Note: Shaded areas represent recessions as defined by the National Bureau of Economics Research.
Source: Grose, Tracey and Patrick Kallerman, "The 1099 Economy – Elusive, but Diverse and Growing", Insights, *Bay Area Council Economic Institute*



Under the current regulatory environment, the sharing economy is "sandwiched between less-regulated private ownership and highly regulated public commerce".[104] Many would argue that sharing economy platforms are facing much less regulation than the companies they are disrupting (taxi unions, hotel chains). Additionally, many fear that classifying service providers as independent contractors may result in fewer benefits and protections (minimum wage, overtime pay, health and life insurance benefits or collective bargaining rights).[105] This has resulted in a number of highly visible battles between incumbents and sharing economy platforms. Some cities have responded to the trend by "issuing cease-and-desist orders, fining platforms, and seeking injunctions", such as New York City and San Francisco, which have launched highly visible campaigns against illegal hotel operators.[106] The success of these efforts has been limited; for example, short-term rental hosts continue to operate illegally in many cities.[107]

Given the regulatory battles, pockets of the sharing economy may show slow growth in the future. However, on a global scale, growth is expected to continue accelerating.

Key risks

The largest threat identified was socio-economic, particularly the erosion of labour benefits including minimum wage, overtime pay and health insurance benefits – a topic widely discussed in the media. This is also why the sharing economy's uptake varies greatly from city to city, state to state and nation to nation.

The World Economic Forum *Global Risks Report 2017* touched on this risk:

This shift [the move to a sharing and collaborative economy] also has negative implications: it means workers can expect more volatility in their earnings and leaves them without the employment protections enjoyed by "standard" employees … New employment models also hinder the collection of taxes from both employer and worker, reducing the amount governments have available to fund social protections.[108]

Implications for the insurance industry

The insurance industry undoubtedly has a role in this market. However, a number of challenges still need to be overcome.

Existing underwriting frameworks may not be adequate for sharing economy policies. Sharing economy firms do not usually have, for example, detailed information on properties or 10 years of loss data. One interviewee on this topic talked in depth about this issue: "When we originally went into the insurance marketplace, we were immediately asked for 10 years of loss data, characteristics of all of our properties, etc. Sharing economies don't know if there is a swimming pool on site, they don't know their proximity to fire stations."

The biggest challenge for incumbents is the absence of credible loss data due to rapid growth. However, one could argue that large sharing economy companies have more actuarially credible data based on what they track than many other mature businesses. Insurers can act on this

opportunity by developing innovative pricing models that may look quite different from what exists today. In some scenarios, taking into account customer feedback, such as the "Uber rating system", could even be imagined.

In addition, the fragmented regulatory environment changes the risk profile across jurisdictions, making it a less unified market and difficult for insurers to underwrite. At the moment, regulation varies by nation, state, municipality and airport jurisdiction. Insurers find it costly to stay abreast of regulation in such a fragmented environment in order to modify coverage as needed throughout the policy term.

Despite the challenges, the sharing economy represents an opportunity for the insurance industry. Large incumbents offer options to insure the personal layer of risk and the commercial layer of risk, but not both together. The protection layer required to ensure the industry's workers, contractors and customers are adequately covered must be defined.

Conclusion

Existing risk mitigation strategies will be most difficult to adapt to risk with a fast risk clockspeed and the potential to pose a significant societal threat (Figure 10). These are the risks with greater scale and uncertainty than others.

According to Keith Smith, Manager, Innovation and Emerging Risks Team, Lloyd's of London, risks with a fast clockspeed will require greater emphasis on principles, creativity and expertise in the future. Rules, detail, consistency and process are those comforts that are only available for risk with slower clockspeed (Figure 11).

The next section of the White Paper highlights how the roles of insurers, governments and technology firms will need to evolve to address the changing risk landscape.

Figure 11: Risk Clockspeed vs Societal Impact Framework

Source: World Economic Forum and Oliver Wyman

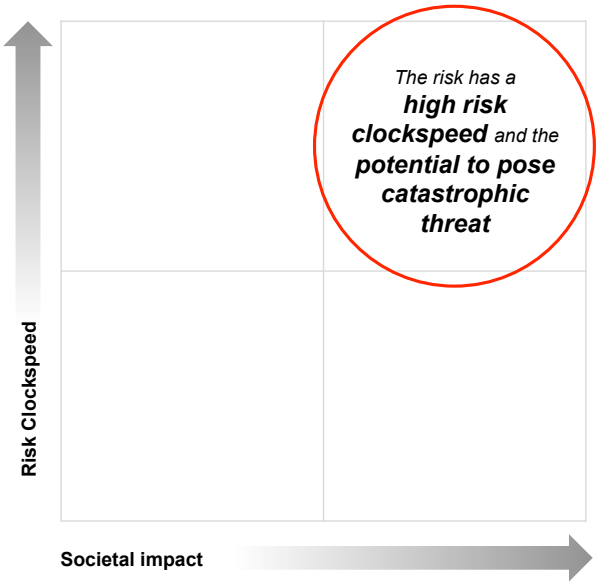
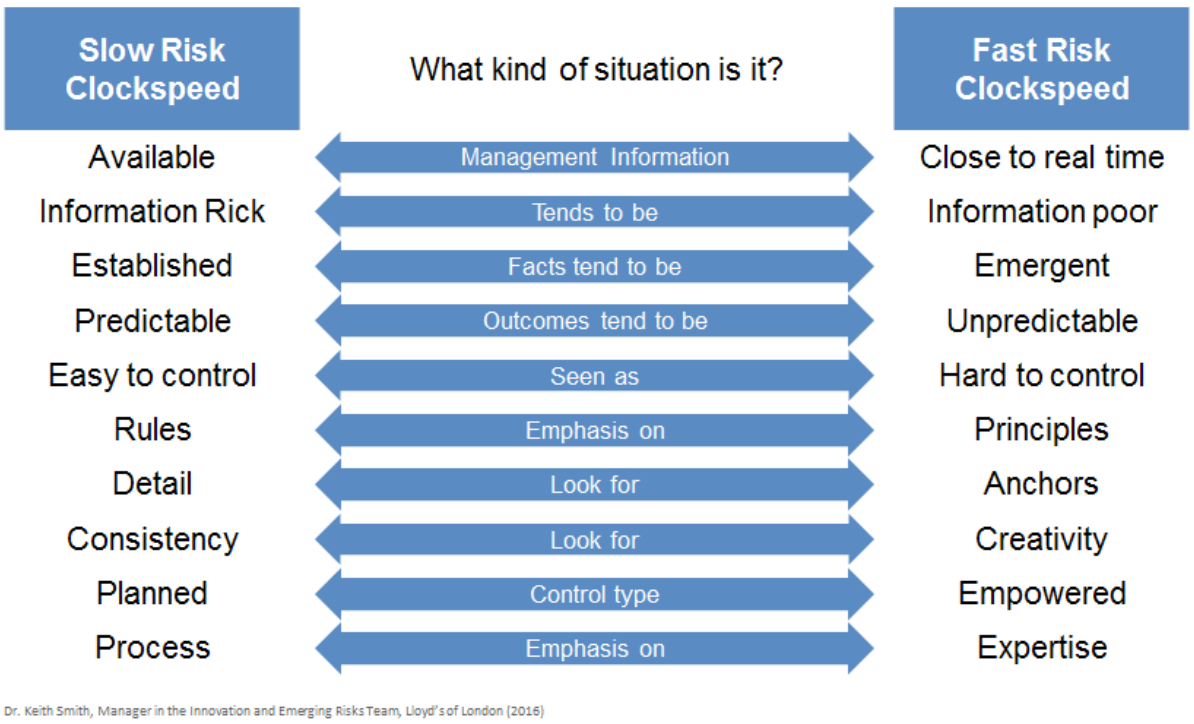


Figure 10: Slow Risk Clockspeed vs Fast RIsk Clockspeed

Source: Keith Smith, Lloyd's of London



Dr. Keith Smith, Manager in the Innovation and Emerging Risks Team, Lloyd's of London (2016)

3. Risk Mitigation in the Innovation Economy

The prior section discussed how governance and legal issues related to emerging technology innovations, including liability, health, safety and data protection, present significant risk management challenges for technology developers, policy-makers and insurers.

Predicting these risks is difficult because of the general technical complexity of emerging technologies and the lack of information about potential damages. Technological standardization and legal certainty is necessary to manage these risk, but these tools tend to lag innovation.

Further complicating the issue is the growing number of stakeholders in an environment where roles and responsibilities are not well defined. Who is responsible for ensuring innovation is safe? Who should take on the new risks of innovation? Who will govern these new innovations? Emerging technologies cross geographical and industry sector boundaries, and no single entity is capable of fully governing these innovations.

The next section highlights how the roles of insurers, governments and technology firms will need to evolve to address the changing risk landscape. These recommendations are intended to enable emerging technologies to serve their intended purpose while minimizing the potential array of negative implications.

"If we take the initiative, maybe we can shape how these one-in-a-million events evolve."

John J. Haley, Chief Executive Officer, Willis Towers Watson, USA

3.1 The evolving role of insurance

Support consumers and businesses to better understand the risks they face

Society currently suffers from a wide and persistent knowledge gap. Consider entrepreneurs concerned about the security of their new smartphones: What strategies can they use to manage this risk? Will a $5 million policy covering reputation or business disruption really be sufficient to put their minds at ease?

The persistence and scale of technology-induced change have led to many questions that remain unanswered. Each technology presents different kinds and levels of risk, each of which depends on how the technology is produced, how it is being used and how it interacts with people. Individuals and businesses have a hard time wrapping their heads around these risks, and the accidents or damages they may cause.

In the case of users concerned about the security of their new smartphones, the real need is a better understanding of these risks. Are they using their smartphones in ways that increase their vulnerability to an attack? Are there specific types of activities they should avoid performing on a smartphone? And what are the actual risks? How likely is the risk of a hack? If a hack occurs, what data are hackers likely to get hold of, and how are they likely to use this data? These are the types of questions that demand answers.

In the past, the insurance industry has largely focused on risk protection, and to some extent risk mitigation. In the future, they have an opportunity to play a larger role in risk education. The industry could close the knowledge gap when it comes to understanding and managing emerging technology risks.

Where can the industry start? Insurers are beginning to better understand what it usually takes to respond to a technology-related event and what safeguards exist to protect against these events. The challenge is getting this information in front of the risk management society in an impactful way. As public or private organizations adopt new technologies, insurers can play an advisory role in supporting them to better understand the risks of emerging technologies and to ensure the appropriate risk management capabilities are in place to manage these new risks. This will remain incredibly important if insurers want to continue to play a risk advisory role in the future.

“The core purpose of the insurance industry is to enable risk-taking, support economic growth and encourage innovation.”

Daniel Glaser, President and Chief Executive Officer, Marsh & McLennan Companies (MMC), USA; Member, Steering Committee

Develop new approaches to measure and assess risk

Notwithstanding the critical role of education, insurance as a risk transfer tool will almost certainly continue to remain important in the future. Leaving the burden of these risks on the government, or on individuals and companies themselves, could jeopardize innovation.

In a society where the relative share of insurable risks declines substantially over time, economic growth will be hampered. Will driverless car technology become the norm if it is impossible to predict and mitigate the risks it poses to society? Will individuals trust their banks if the risk of cyberattacks on large institutions becomes too great? Serious societal repercussions might follow without a protection blanket to mitigate or transfer emerging risks.

In the past, historical data-driven models have been more or less effective in analysing risk. For natural catastrophe risks, for example, meteorological and seismological indicators offer some relative sense of predictability. Similarly, factors such as driving history, car type and colour have been effective in assessing the risk of future automobile crashes. According to Thomas Wilson, Chief Risk Officer, Allianz SE, Germany, three critical assumptions underlie data-driven risk models:[109]

1. Sufficient past data are available to characterize the uncertainty
2. Past developments are a good representation of future uncertainty
3. A direct and predictable link exists between the modelled events and their impact on measures of interest

A number of reasons can explain why these underlying assumptions may not apply to emerging technology risks.

First, the availability of insured-level data on some of these risks remains an important gap.

Second, given the rapidly changing technological environment, events rarely arise from the same conditions. By their definition, many of these events are considered “black swans”.[110] Any accurate quantification needs to be dynamic and constantly adapting to new developments and progress.

Third, scenarios of this magnitude tend to trigger a series of cascading events that are almost impossible to predict. The failure of the electricity grid, for example, may disrupt other critical national infrastructure, given the interdependencies across systems.

The lack of historical data will require alternative sources of information to better understand emerging technology risks. “What the industry needs is data, and analytics to translate statistics on losses into [consistent pricing].”[111]

In addition to alternative data sources, insurers may consider new forms of modelling for these emerging risks, where “past losses and patterns may not necessarily be indicative and directly applicable to future emerging threats”.[112]

Open-source platforms, for example, may support the industry in these undertakings. The Oasis Loss Modelling platform is the first of its kind in this field. The platform is fully open source, allowing “independent developers to create and input various hazards, vulnerability and exposure elements”.[113] Many believe that such open-source platforms “will lower the barrier of entry for academics and small specialist teams on innovating and developing models that will create more credible views of overall risk and the ever increasing number of emerging perils and cat risk”.[114]

Insurers will need to continue to innovate in this area to ensure they are capable of responding, especially as black swan events grow in scale, significance and frequency.

“The insurance industry can harness new technologies to measure and assess risk, supporting the success of new business ideas.”

Dieter Wemmer, Chief Financial Officer, Allianz, Germany; Member, Steering Committee

Address protection gaps and unmet needs

Insurance companies have enabled society to tackle most new risks with a well-established iterative approach. In the beginning, they are conservative in their underwriting assumptions. Over time, as they better understand the risk profile from claims data, they revise pricing models and ultimately offer affordable insurance protection.

This model will be difficult to adopt for the new challenges ahead. Numerous emerging risks are of greater scale and uncertainty than prior ones. Such uncertainty makes assessing risk difficult, potentially leading to delays in large-scale adoption or to higher prices. This is already seen in the commercial drone market, as some demand currently exists for drone insurance. However, brokers claim they have had difficulty placing the business. The aviation market covers damage to the drone itself, but not exposure to third-party liability or personal injury.

A similar case can be made for self-driving vehicles. Tesla, a leader in driverless car technology, has discussed this issue publicly. On a recent earnings call, Jon McNeill, President, Global Sales and Service, Tesla Motors, USA, explained that "in Asia, the majority of Tesla cars are sold with an insurance product that is customized to Tesla, that takes into account not only the Autopilot safety features but also the maintenance costs of the car".[115] Elon Musk, Chairman, Tesla Motors, USA, insists that this is not intended to disrupt the insurance market. Instead, many are seeing this as a move to urge insurers to start thinking ahead. "If we need to we'll insource it," he said of the included insurance plan, "but I think we'll find that insurance partners do adjust rates proportionate to the risk of a Tesla."[116]

In the future, insurers should look to uncover and ultimately address protection gaps and unmet needs. At times this may require investment in product development or innovation hubs to harness digital innovation, and advanced analytics to deliver new solutions.

If incumbents don't act now, niche players may step in to fill the gap. Some have already emerged in the sharing economy area (SafeShare), where they perceive a lack of available solutions in the current market. Others may emerge if the insurance industry is not able to stay abreast of the changing technology and risk landscape.

3.2 The evolving role of government

Start with guidance rather than rule-making

The governance of emerging technologies is patchy; some are regulated heavily, and others hardly at all, with many gradients of oversight between these ends of the spectrum. The lack of clarity around governance and legal issues related to emerging technology innovations is presenting significant risk management challenges for technology developers, technology deployers and insurers. In an era of rapid change, governments are struggling to understand how emerging technologies are used, let alone to regulate their use. Some forward-thinking governments have navigated these challenges by first establishing a foundation and a framework upon which future governmental action will occur. By providing markets with their latest thinking on an emerging issue, governments are able to give markets the heads up before introducing a new rule.

For example, the US Food and Drug Administration (FDA) recently issued a set of recommendations on health and lifestyle wearables. As stated in the recommendations, "[the] FDA's guidance documents … do not establish legally enforceable responsibilities. Instead, guidances describe the Agency's current thinking on a topic".[117] These guidelines provide examples of how new devices would be evaluated by the FDA. Technology players developing new health wearable products, for example, can use these guidelines to determine how to proceed before getting FDA approval for their devices.[118]

Similarly, in 2016, the US Department of Transportation (DOT) released policy which set out an ambitious approach to accelerate the highly automated vehicle (HAV) revolution. The policy was released as "agency guidance rather than in a rulemaking in order to … guide manufacturers and other entities in the safe design, development, testing, and deployment of HAVs".

The federal guidelines were welcomed by automobile manufacturers. Before this, no one was quite sure how autonomous vehicles were going to be regulated, or what software or data requirements they would need.[120] This was an effort by the DOT to recognize that automobile manufacturers need guidance on what is expected of them. Many praised the DOT for the progressive action. "The agency has pretty deftly walked a middle path, offering guidance substantial enough to bring some clarity to the market but broad enough to allow for plenty of innovation and competition."[121]

These guidelines allow for early engagement with technology and product providers, as well as early consultation with consumers.

"We need to find an effective way to allocate these new risks, because if the risk simply falls on the government, there will be a knee-jerk reaction to overregulate."

Alan D. Cohn, Adjunct Professor, Georgetown University Law Center, USA

Consider using "policy sandboxes" to get ahead of the governance challenge

Developing new policies requires time. In the meantime, governments can accelerate the development and use of "regulatory sandboxes" to get ahead of the governance challenge.

What is a regulatory sandbox? Today, it exists mainly in the banking sector, under the term "fintech sandbox". The idea is that regulators will relax specific legal and regulatory requirements, which the "sandbox" entity will otherwise be subject to for its duration. This allows emerging fintech companies to get off the ground and focus on generating a revenue stream without running into regulatory and legal barriers from the outset.

Over the last year, regulators around the globe have come forward to establish fintech sandboxes, including the Australian Securities and Investments Commission (March), the Monetary Authority of Singapore (June), the Bank of Thailand (September) and the Hong Kong Monetary Authority (September). Also in 2016, the Financial Authority in the United Kingdom, one of the first regulatory bodies to adopt the sandbox approach, began accepting applications for its first cohort.

The key objective of these sandboxes is for regulators to educate themselves on new ideas. In that respect, the concept can be used in a number of ways in other areas of the economy, specifically to experiment with the impact of different regulatory regimes on emerging technologies.

3.3 The evolving role of technology players

Show up to the table

Without doubt, technological advances are bringing seamless benefits to society. However, the disruptive nature of such advances has led to a significant amount of friction between governments and the technology industry over the years.

Technology players need to recognize that the speed of technological innovation is creating significant challenges for governments, and they must find ways to help limit the negative externalities.

Technology players should start thinking of themselves not only as innovators, but also as stakeholders in shaping the future of risk mitigation. The technology industry has deep knowledge, data science and related risk expertise. As experts in this area, the industry's players have the opportunity and responsibility to take on a larger role in supporting the development of risk mitigation solutions. Who is better positioned to collaborate on the development of industry standards than the technology industry itself? The industry is a critical player in building a society against risks stemming from its own innovations.

"I actually think this is a problem we [as the technology players and insurers] can work on together. Yes, there are new risks, but there are also new ways of understanding these risks."

David Kenny, Senior Vice-President, IBM Watson, IBM Corporation, USA

Case study: State of standards for the internet of things

The security of IoT devices has not kept up with the rapid pace of adoption, creating substantial safety and operational risks. IoT devices lack comprehensive, widely adopted international norms and standards for IoT security. For example, many IoT devices might be deployed in circumstances that make it difficult to upgrade them, or devices may have no clear way of alerting users when a security problem arises.

In the United States, the President's National Security Telecommunications Advisory Committee made the following statement regarding this issue in 2014:
IoT adoption will increase in both speed and scope, and [will] impact virtually all sectors of our society. The Nation's challenge is ensuring that the IoT's adoption does not create undue risk. Additionally … there is a small – and rapidly closing – window to ensure that IoT is adopted in a way that maximizes security and minimizes risk. If the country fails to do so, it will be coping with the consequences for generations.[122]

In the case of the IoT, the technology industry is spearheading efforts to develop standards. Many collaborative efforts led by Google, Intel, Qualcomm and GE, for example, are in the race to establish standards for the industry.

3.4 The evolving role of risk owners

Consider the risks

For the purposes of this White Paper, risk owners are defined as the companies or consumers that adopt and deploy new innovations. They are not the developers themselves, but the deployers and users of new technologies. These stakeholders have their own responsibility in light of this changing risk landscape.

Consider an event in February 2017, when Amazon's S3 cloud storage system went down, causing large disruptions across the internet. Interestingly, Amazon itself was not affected by the outage. The company was likely spared because "they have designed their sites to spread themselves across multiple Amazon geographic zones, so if a problem comes up in one zone, it doesn't hurt them".[123] In the future, other companies may follow this practice to help reduce the risk themselves.

According to the Marsh and RIMS 14th Annual Excellence in Risk Management Report, "Too many organizations don't realize the pervasiveness of some technologies, [including] telematics, sensors, and the IoT"[124] within their organizations. The study found that "the inability to model the magnitude of disruptive technology risks … undoubtedly contributes to the lack of focus on them … Improving organizational risk alignment should include investment in the resources that give risk executives the additional bandwidth to stay on top of the accelerated pace of new and emerging risks."[125]

Consumers and companies will need to find a balance in the future between adopting new innovations in an unrestricted way and taking the time to first understand the potential consequences they may cause. As already discussed, the insurance industry may play an important advisory role in facilitating these discussions.

3.5 Global dialogue to strengthen the outcome

Emerging risks are shared by society, and there is little advantage in tackling the issue alone. Significant dialogue will be required between various parties – governments, businesses, insurers and technology companies – and across borders to mitigate these new risks.

Finding a common understanding of the issue is the first step to finding a solution. Rachel Haot, Chief Digital Officer (2011-2013), City of New York, USA, emphasized this point: "It's hard to align interests if siloed stakeholders across government, technology, and business aren't interacting or even speaking the same language."[89]

Over the course of this work, three areas in particular were identified where a common understanding of the issue was needed to drive the discussion forward.

The first is liability. Existing rules were not designed with autonomous systems in mind, which has left stakeholders – from users to developers to deployers – guessing as to how current liability rules will be applied in practice.

The second is data. The exchange of data can and will be an effective tool to support the management of vulnerabilities and threats. However, consensus on who owns data sources and who should have access to them is lacking

The third is standards, which govern the design, construction, operation and use of nearly everything produced. However, it is difficult to write requirements for an application, use or need that either does not yet exist, or does but only marginally.

"If we let these products emerge on their own, the risks will become so big that we will not be able to handle them."

Inga Beale, Chief Executive Officer, Lloyd's, United Kingdom

Support the development of new approaches to handle liability in practice

Products and services are regulated by existing liability rules which, unless proven otherwise, still apply. Unfortunately, existing rules were not designed with complex and autonomous systems in mind. Thus, anticipating the way they will be applied in practice is not easy. Under existing product rules, the user is required to prove that damage has been caused by a product defect. As these technologies become increasingly complex, it will be ever more difficult to assess "what went wrong" and, therefore, very challenging for a user to prove a product defect. In many ways, the user will be faced with an almost impossible burden of proof.

Similarly, manufacturers are faced with a number of outstanding questions. Under several theories of liability, manufacturers can be held responsible for systems which leave the user in total or partial control, under the claim that users were misinformed about the system's true capabilities. To avoid the risk of liability, manufacturers may be incentivized to understate system capabilities during advertising and even to deactivate the technology if the user appears to be inattentive. For example, autopilot features in cars require owners to keep their hands on the wheel and their eyes on the road at all times. It is not hard to imagine autonomous vehicles in the future ringing alarms if they sense their drivers are distracted.

Further complicating matters are potentially expensive mistakes. The GM ignition-switch recall amounted to $4.1 billion in losses in 2014,[127] and Volkswagen's diesel emissions scandal is expected to cost over $7 billion.[128] Punitive damages for designing or manufacturing a defective product can also be significant; a case concerning burns from McDonald's hot coffee led to a punitive damage award of $2.7 million.[129]

In other industries, service-level agreements absolve the technology provider of any substantial liability (e.g. cloud service providers). However, many argue that this may be unsustainable in the future, and that existing service-level agreements may not stand up in the court of law.
This uncertainty regarding the application of liability rules in practice is making it difficult to assess risk. Future litigation and liability disputes could be costly and consume a significant amount of the industry's time and resources.

"Could this uncertainty lead to a gigantic waste of economic resources?"

Andrea Bertoloni, Assistant Professor of Private Law, Scuola Superiore Sant'Anna, Italy

Insurers, governments and technology players need to come together to accelerate the development of a solution to this large and pressing issue. The lack of clear liability rules regarding autonomous systems is one of the biggest barriers to advancing these technologies in the future. One option is to align across industries on a principle-based framework for evaluating liability in practice. This would, to some extent, separate human from machine error and establish the required evidence needed to support the case (e.g. black box data). Another option is to consider a government backstop to limit the total financial liability obligation borne by one industry. This would allow technology companies to produce new products and the insurance industry to cover them, without risking system's collapse in testing phases.

Make alternative sources of information accessible and usable

The exchange of data is an effective tool to support the management of vulnerabilities and threats. In terms of cyber, both the UK and US governments have publicly recognized the need for better data sharing across public and private sectors.[130]

A number of sources of information from government agencies in the United Kingdom have been made available via data feeds, such as the Cyber Security Information Sharing Partnership (CiSP).[131]

In the United States, the Department of Homeland Security is bringing together companies across insurance and other industries to discuss setting up a "third-party repository" for cyber incident information.[132] The working group specifically identified the value of a repository in better understanding "both the immediate and long-term impacts and consequences of cyber incidents."[133] In particular, repository-enabled analyses that show "the cascading effects from a particular kind of cyber incident to be a frequent and/or likely occurrence" could be used to boost the insurer case for addressing supplier and vendor cybersecurity as a condition for insurance coverage.[134]

This exchange of information will serve two purposes. The first is to support governments and societies in better understanding these risks and eventually driving greater resilience against them. The second is to support the insurance industry in building risk models that allow for developing insurance policies and risk management solutions to address these risks.

In the future, governments should continue to foster collaboration and the sharing of information between the public and private sectors. Insurers and technology players should take an active role in these initiatives.

Promote the harmonization of global protocols

Standards are increasingly becoming an important part of people's lives. They govern the design, construction, operation and use of nearly everything produced. They ensure the safety and quality of products, enable interoperability across systems and facilitate international trade.[135] Standards are also helpful in managing risks by helping to limit liability for products meeting those standards. Without them, users (and insurers) have no way of knowing if security or safety was built into new devices.

A patchwork of standards and regulations is likely to ensue if there is no collaboration across borders. The risk from this is an environment in which new technologies must operate under an inconsistent set of safety and operational protocols globally.

It is important to identify areas with significant gaps and promote the development of collaborative efforts to establish global protocols. To accelerate this development, nations can "adopt standards, conventions and model laws" that market leaders have already implemented.[99] The Vice-President of India, Shri M. Hamid Ansari, endorsed this point in a recent lecture on the topic:

We need to be more active in the global standards setting forums and adopt these standards. Adoption of global standards will improve our productivity and enable Indian companies to access the global export market … Even where we employ country specific standards, we must ensure that these equal or better the existing international ones; otherwise we would only be discouraging innovation, and offering to our domestic market, products and technologies that are inferior.[136]

4. A Call to Action: Seek Ways to Accelerate This Revolution and Not Hinder It

“We need to accelerate the development of the required governance and liability systems to ensure the opportunity for civil society and the private sector is not lost.”

Mike McGavick, Chief Executive Officer, XL Group, USA

The issues discussed in this White Paper are some of the biggest barriers to the advancement of new and emerging technologies. Early movers will set the path for the future of this revolution.

The preceding section evoked the need for greater dialogue to reshape approaches to risk resilience in this rapidly changing world. The insurance industry can take the first step towards advancing these discussions.

The industry is often consulted far too late in the dialogue, rather than being involved in the design and planning stages where change can reasonably take place. For insurers to be enablers of the Fourth Industrial Revolution, they will need to simultaneously harness it, developing new solutions to understand the risks while working with governments, technology players and other industries to incentivize greater risk-mitigating behaviour from the bottom up.

The World Economic Forum and Oliver Wyman hope this White Paper can stimulate further discussion and, where appropriate, prompt innovation among insurers, governments and technology players to help mitigate risk and improve resilience.

The first phase of the Mitigating Risks in the Innovation Economy initiative ended with the call to action to seek ways of accelerating this revolution and not hindering it. The initiative’s next phase will focus on convening key stakeholders across the public and private sectors to catalyse action and encourage international collaboration to create market-based solutions that build resilience.

Acknowledgements

Additional contributors

Markus Aichinger, Senior Risk Manager, Allianz, Germany

James Anderson, Director, Institute for Civil Justice, and Senior Behavioral Scientist, RAND Corporation, USA

Nicolas Berg, Head, Liability and Financial Lines, Europe, American International Group (AIG), USA

Andrea Bertoloni, Assistant Professor of Private Law, Scuola Superiore Sant'Anna, Italy

Neeraj Bharadwaj, Director, Peridot Energy Services, India

David Bojanini, Chief Executive Officer, Grupo Sura, Colombia

Andreas Bradt, Project Manager, Automotive Innovation Centre, Allianz Global Automotive, Allianz SE, Germany

Hans-Christoph Burmeister, Group Leader, Sea Traffic and Nautical Solutions, Fraunhofer Center for Maritime Logistics and Services, Germany

Jan R. Carendi, Senior Adviser, Sompo Holdings, Japan

Paul Chong, Director, Watson Group, EMEA, IBM Corporation, USA

Carlo Cimbri, Chief Executive Officer, Unipol Gruppo Finanziario, Italy

Alan D. Cohn, Adjunct Professor, Georgetown University Law Center, USA

Andrew Collinge, Assistant Director, Greater London Authority, United Kingdom

Julien Combeau, Head, Europe, Liability Risk Consulting, American International Group (AIG), USA

James Crawford, Founder and Chief Executive Officer, Orbital Insight, USA

Martin Curley, Vice-President and Director, Intel Labs Europe, Intel Corporation, United Kingdom

Eric David, Co-Founder and Chief Strategy Officer, Organovo, USA

Thabo Dloti, Chief Executive Officer, Liberty Holdings, South Africa

Daniel Dykes, Vice-President, Business Development, Aeon Labs, United Kingdom

Ina Ebert, Leading Expert, Liability and Insurance Law, Munich Re, Germany

Gretchen Effgen, Vice-President, Global Partnerships, nuTonomy, USA

Paul Egan, Principal Consultant, IoTUK, Hardware and Communications, Digital Catapult, United Kingdom

John Elkington, Executive Chairman and Co-Founder, Volans, United Kingdom

Volker Eutebach, Manager, Business Development, Germany and Austria, Lloyd's, United Kingdom

Sophie Evans, Programme Director, Capital, Science and Policy Practice, Willis Towers Watson, United Kingdom

Kevin Farrell, Chief Product Officer, TrueMotion, USA

Jerome Ferguson, Director, Autonomous Systems, United Postal Service (UPS), USA

John Flint, Chief Executive, Retail Banking and Wealth Management; Group Managing Director, HSBC Bank, United Kingdom

Craig Foster, Managing Director, HomeServe Labs, United Kingdom

David Gann, Vice-President, Innovation, Imperial College London, United Kingdom

Jonathon Gascoigne, Senior Risk Adviser, Capital, Science and Policy Practice, Willis Towers Watson, United Kingdom

Nicholas Gibbs, Assistant Liability Underwriter, Apollo Syndicate Management, United Kingdom

Daniel Glaser, President and Chief Executive Officer, Marsh & McLennan Companies (MMC), USA

Anne Glover, Chief Executive Officer, Amadeus Capital Partners, United Kingdom

Caroline Gorski, Head of Internet of Things – IoTUK, Digital Catapult, United Kingdom

Randall Harbert, Executive Vice-President; Chief Agency Sales and Marketing Officer, State Farm Mutual Automobile Insurance Company, USA

Pierre Hausemer, Founder and Partner, VVA Europe, United Kingdom

Jose Heftye, Managing Director, Sharing Economy Practice Leader, Marsh, USA

Ede Jorge Ijjasz, Senior Director, Social, Urban, Rural and Resilience Global Practice, World Bank, Washington DC

Peter Irvine, Associate Director, Office of Aviation Analysis, US Department of Transportation, USA

Ajit Jaokar, Director, AI for Smart Cities Lab, University of Madrid, Spain

Richard Jinks, Manager, Facilities Centre of Excellence, XL Catlin, United Kingdom

Bjoern Juretzki, Policy Officer, European Commission, Brussels

Bruce Katz, Vice-President and Director, Metropolitan Policy Program, Brookings Institution, USA

Steve Kempsey, Head, Casualty, Marsh, USA

David Kenny, Senior Vice-President, IBM Watson, IBM Corporation, USA

Anne Kilgallon, Vice-President, Enterprise Strategy and Innovation, American Association for Retired Persons (AARP), USA

Keiji Kojima, Chief Executive Officer, Services and Platforms; Senior Vice-President and Executive Officer, Hitachi, Japan

Mirko Kovac, Director, Aerial Robotics Lab, Imperial College London, United Kingdom

Ulrike Leyherr, Head, PC Centre of Competence, Allianz, Germany

Ole Lund Hansen, Chief, Business of Tomorrow, United Nations Global Compact, New York

Andrew McAfee, Principal Research Scientist, MIT Initiative on the Digital Economy, Massachusetts Institute of Technology (MIT), USA

Mike McGavick, Chief Executive Officer, XL Group, USA

Andreas Mai, Director, Product Management Smart Connected Vehicles, Cisco, USA

Johanna Mair, Professor of Organization, Strategy and Leadership, Hertie School of Governance, Germany

Benita Matofska, Chief Sharer, The People Who Share, xxx

Andrew Maynard, Professor, School for the Future of Innovation in Society, Arizona State University, USA

Kevin Meagher, Senior Vice-President, Business Development, ROC Connect, United Kingdom

Atul Mehta, Global Head, Telecom Media Technology, Venture Capital and Funds, International Finance Corporation, Washington DC

Anil Menon, Global President, Smart+Connected Communities, Cisco Systems, India

Pascal Millaire, Vice-President and General Manager, Cyber Insurance, Symantec Corporation, USA

Kevin O'Donnell, President and Chief Executive Officer, RenaissanceRe Holdings, Bermuda

Günther H. Oettinger, Commissioner, Budget and Human Resources, European Commission, Brussels

Sandip Patel, Global Managing Director, Insurance Industry, IBM Corporation, USA

Brian Peccarelli, President, Tax, Accounting, Thomson Reuters, USA

Alan Penn, Dean, Bartlett, University College London, United Kingdom

Monica Pesce, Managing Director, VVA Brussels, Belgium

Cristiano Pizzocheri, Chief Technology Officer and Co-Founder, SafeShare, United Kingdom

Stephen Prior, Reader in Unmanned Air Vehicles, University of Southampton, United Kingdom

Carlo Ratti, Director, SENSEable City Laboratory, MIT - Department of Urban Studies and Planning, USA

Monica Rivas Casado, Lecturer in Applied Environmental Statistics, Cranfield Institute for Resilient Futures, Cranfield University, United Kingdom

Richard Roberts, Project Breakthrough Fellow, Volans Ventures, United Kingdom

Adam Sager, Chief Executive Officer and Co-Founder, Canary, USA

Kate Sampson, Vice-President, Risk Solutions, Lyft, USA

Daniel Schreiber, Chief Executive Officer, Lemonade, USA

John Schultz, Executive Vice-President, General Counsel and Corporate Secretary, Hewlett Packard Enterprise, USA

Thomas Schumann, Senior Internal Auditor, Allianz, Germany

Thomas Sedran, Senior Vice-President, Group Strategy, Volkswagen, Germany

Ole Sieverding, Product Head, Cyber and Data Risks, Hiscox, Germany

Ingvild Soerensen, Senior Manager, Global Compact LEAD, United Nations Global Compact, New York

Alexander Steinart, Chief Executive Officer and Co-Founder, SafeShare Global, United Kingdom

Ramy Tadros, Partner, Financial Services, Oliver Wyman (MMC), USA

Daniel Veit, Professor, Faculty of Business and Economics, University of Augsburg, Germany

Jerry Velasquez, Chief of Section; Head, Making Cities Resilient Campaign, United Nations International Strategy for Disaster Reduction (UNISDR), Geneva

Mario Verdicchio, Assistant Professor, Computer Science, University of Bergamo, Italy

Jonny Voon, Innovation Lead, Digital (IoT and Blockchain), Innovate UK, United Kingdom

Bryant Walker Smith, Assistant Professor of Law, University of South Carolina, USA

Juergen Weichert, Head, Global Product Development Liability, Allianz, Germany

Niklas Weiler, Project Lead, Renewable Energy, Allianz, Germany

Brian Witten, Senior Director, Symantec Research Labs Worldwide, Symantec Corporation, USA

Jim Wood, Director, IT and Information Services, London Legacy Development Corporation, United Kingdom

Eric Woods, Research Director, Navigant Consulting, USA

Note: Positions listed at the time of contribution.

Endnotes

1. Berman, Alison and Jason Dorrier, "Technology Feels Like It's Accelerating — Because It Actually Is", *Singularity Hub*, March 2016, https://singularityhub.com/2016/03/22/technology-feels-like-its-accelerating-because-it-actually-is/.
2. Kurzweil, Ray, "The Law of Accelerating Returns", 2001, http://www.kurzweilai.net/the-law-of-accelerating-returns.
3. Ibid.
4. Sneed, Annie, "Moore's Law Keeps Going, Defying Expectations", *Scientific American*, May 2015.
5. Smith, Keith, "Risk Clockspeed: An Introduction to Risk Clockspeed", Institute of Risk Management Forum, April 2010.
6. National Academy of Sciences, *Preparing for the 21st Century: Technology and the Nation's Future*, 1997.
7. World Economic Forum, op. cit.
8. Associated Press, "Growing dependence on technology raises risks of malfunction", *Crain's New York Business*, July 2015, http://www.crainsnewyork.com/article/20150709/TECHNOLOGY/150709895/growing-dependence-on-technology-raises-risks-of-malfunction.
9. https://www.preqin.com/docs/newsletters/inf/Preqin_INFSL_Feb_2013_Insurance_Companies_Investing.pdf >>
10. Axelrod, C. Warren, *Managing the Risks of Cyber-Physical Systems*, 2013.
11. Condliffe, Jamie, "Amazon's $150 Million Typo Is a Lightning Rod for a Big Cloud Problem", *MIT Technology Review*, March 2017, https://www.technologyreview.com/s/603784/amazons-150-million-typo-is-a-lightning-rod-for-a-big-cloud-problem/.
12. Ibid.
13. https://www.preqin.com/docs/newsletters/inf/Preqin_INFSL_Feb_2013_Insurance_Companies_Investing.pdf >>
14. Lloyd's and University of Cambridge Centre for Risk Studies*, Business Blackout: The insurance implications of a cyber attack on the US power grid*, Emerging Risk Report – 2015.
15. Harvey, Tom, "Prudential Regulation Authority on the Challenges Facing Cyber Insurers", Risk Management Solutions (RMS), http://www.rms.com/blog/2016/11/22/prudential-regulation-authority-on-the-challenges-facing-cyber-insurers/.
16. Ibid.
17. Ibid.
18. Smith, op. cit.
19. Goldman Sachs Global Investment Research, *Drones: Flying into the Mainstream*, Profiles in Innovation, March 2016.
20. Apex Insights, "About the Global Parcel Delivery Market Insight Report 2017", https://www.apex-insight.com/product/global-parcel-delivery-market-insight-report-2017/.
21. Ibid.
22. Ibid.
23. Lardinois, Frederic, "Amazon starts Prime Air drone delivery trial in the UK – but only with two beta users", *TechCrunch*, December 2016, https://techcrunch.com/2016/12/14/amazons-prime-air-delivery-uk/.
24. Reisinger, Don, "Watch Amazon's Prime Air Complete Its First Drone Delivery", *Fortune*, December 2016, http://fortune.com/2016/12/14/amazon-prime-air-delivery/.
25. Smith, Alexander, "Drone Has 'Very Near Miss' With Airbus Jet Near The Shard in London", *NBC News*, November 2016, http://www.nbcnews.com/news/world/drone-has-very-near-miss-airbus-jet-near-shard-london-n685261.
26. Vincent, James, "The UK government is crashing drones into airplanes to see what happens", *The Verge*, October 2016, http://www.theverge.com/2016/10/18/13314916/drone-crash-airplane-test-uk-dangers.
27. Ibid.
28. The Robotics Institute, "Navlab: The Carnegie Mellon University Navigation Laboratory", http://www.cs.cmu.edu/afs/cs/project/alv/www/index.html.
29. Bradshaw, Tim, "Self-driving car numbers double on California roads", *Financial Times*, March 2017, https://www.ft.com/content/4377b4c0-0479-11e7-aa5b-6bb07f5c8e12.
30. Ibid.
31. Kokalitcheva, Kia, "Uber's Self-Driving Car Plans Involve a Trucking Startup", *Fortune*, August 2016, http://fortune.com/2016/08/18/uber-otto-acquistion/.
32. Davies, Alex, "The Numbers Don't Lie: Self-Driving Cars Are Getting Good", *Wired*, February 2017, https://www.wired.com/2017/02/california-dmv-autonomous-car-disengagement/.
33. Ibid.
34. Smith, Bryant Walker, "How Governments Can Promote Automated Driving", *New Mexico Law Review*, March 2016.
35. Simonite, Tom, "Prepare to be Underwhelmed by 2021's Autonomous Cars", *MIT Technology Review*, August 2016, https://www.technologyreview.com/s/602210/prepare-to-be-underwhelmed-by-2021s-autonomous-cars/.
36. Dowling Report IBNR No. 36, September 2013.

37. Vincent, James, “Apple boasts about sales; Google boasts about how good its AI is”, *The Verge*, October 2016, http://www.theverge.com/2016/10/4/13122406/google-phone-event-stats.

38. Ibid.

39. Lewis-Kraus, Gideon, “The Great A.I. Awakening”, *The New York Times Magazine*, December 2016, https://www.nytimes.com/2016/12/14/magazine/the-great-ai-awakening.html?_r=1.

40. Waral, Jitendra, Anurag Rana and Sean Handrahan, “Artificial intelligence: Disruption era begins*”, Bloomberg Intelligence*, September 2016, https://www.bloomberg.com/professional/blog/artificial-intelligence-disruption-era-begins/.

41. Ibid.

42. Ibid.

43. Bergen, Mark, “Google’s AI Hasn’t Passed Its Biggest Test Yet: Hunting Hate”, *Bloomberg Technology*, March 2017, https://www.bloomberg.com/news/articles/2017-03-31/google-s-ai-hasn-t-passed-its-biggest-test-yet-hunting-hate.

44. Ibid.

45. Ibid.

46. Cambridge Centre for Smart Infrastructure and Construction, *Smart Infrastructure: Getting more from strategic assets*, 2017.

47. Ibid.

48. Peleg, Amir, “Investment in Smart Water Systems on the Rise”, *Civil + Structural Engineer*, May 2014, http://csengineermag.com/article/investment-in-smart-water-systems-on-the-rise/.

49. European Commission, “Smart grids and meters”, https://ec.europa.eu/energy/en/topics/markets-and-consumers/smart-grids-and-meters.

50. Ibid.

51. Schneider, Reto, *Priorities of the insurance industry with respect to emerging risks*, Swiss Re, 2015.

52. Lloyd’s and University of Cambridge Centre for Risk Studies, op. cit.

53. Ibid.

54. Kharif, Olga, “The Internet of Things: When Toasters Go Online”, *Bloomberg Quick Take*, October 2016, https://www.bloomberg.com/quicktake/internet-things.

55. International Data Corporation (IDC), *Fitness Trackers in the Lead as Wearables Market Grows 3.1% in the Third Quarter, According to IDC* [Press release], December 2016, https://www.idc.com/getdoc.jsp?containerId=prUS41996116.

56. Ibid.

57. Berg Insights, *Smart Homes and Home Automation*, M2M Research Series, http://www.berginsight.com/ReportPDF/ProductSheet/bi-sh4-ps.pdf.

58. Ibid.

59. Ibid.

60. Vázquez, Juan Ignacio, “Outlook for the Internet of Things”, *MIT Technology Review*, October 2016, https://www.technologyreview.com/s/602114/outlook-for-the-internet-of-things/.

61. Ibid.

62. Gupta, Vibhoosh, “The Emerging Industrial App Economy”, GE, https://www.ge.com/digital/blog/emerging-industrial-app-economy.

63. TRAXA, “Report: Industrial Internet of Things (IIoT) in China, where is the Growth?”, August 2016, an overview of the report *Growing From Big to Strong: A Pragmatic Assessment of Industry 4.0 Challenges and Opportunities in China*, published by IoT ONE1 and STM Stieler1, http://www.traxa.it/en/news-en/report-industrial-internet-of-things-iiot-in-china-where-is-the-growth/.

64. “Chinese Firm Says Its Cameras Were Used to Take Down Internet”, *Bloomberg News*, October 2016, https://www.bloomberg.com/news/articles/2016-10-24/chinese-firm-says-its-cameras-were-used-to-take-down-internet.

65. Ibid.

66. State Farm, “Canary: The All-In-One Security System for Any Home”, https://www.statefarm.com/customer-care/life-events/smart-home-systems/canary.

67. American Family Insurance, “Ring Protects What Matters Most”, https://myapps.amfam.com/amfamring/#/landing.

68. Higginbotham, Stacey, “Why Insurance Companies Want to Subsidize Your Smart Home”, *MIT Technology Review*, October 2016, https://www.technologyreview.com/s/602532/why-insurance-companies-want-to-subsidize-your-smart-home/.

69. Telles Jr., Rudy, *Digital Matching Firms: A New Definition in the “Sharing Economy” Space*, US Department of Commerce – Office of the Chief Economist, 2016.

70. Ibid.

71. Ibid.

72. Ibid.

73. Grose, Tracey and Patrick Kallerman, “The 1099 Economy – Elusive, but Diverse and Growing”, Insights, *Bay Area Council Economic Institute*, http://www.bayareaeconomy.org/the-1099-economy%E2%80%8A/.

74. Ibid.

75. Ibid.

76. Katz, Vanessa, “Regulating the Sharing Economy”, *Berkeley Technology Law Journal*, Volume 30, Issue 4, November 2015.

77. Ibid.

78. Ibid.

79. Ibid.

80. World Economic Forum, op. cit.

81. Wilson, Thomas, “Risk Management in an Increasingly Complex and Interconnected World”, *Glocalism*, 3, 2015.

82. Guy Carpenter, *Ahead of the Curve: Understanding Emerging Risks*, Emerging Risks Report September 2014, Marsh & McLennan Companies, 2014.

83. Mullaney, Tim, “Can We Insure the Internet of Things Against Cyber Risk?”, *MIT Technology Review*, January 2016, https://www.technologyreview.com/s/545736/can-we-insure-the-internet-of-things-against-cyber-risk/.

84. Guy Carpenter, “The Rise of Emerging Risk and Casualty Catastrophe Models”, at *gccapitalideas.com*, December 2015.

85. Guy Carpenter, 2014, op. cit.

86. Ibid.

87. Morse, Jack, “Tesla is so sure its cars are safe that it now offers insurance for life”, *Mashable*, February 2017, http://mashable.com/2017/02/23/elon-musk-tesla-lifetime-insurance/#uYPLmBieTkq3.

88. Ibid.

89. Pontin, Jason, “Why Tech Companies Should Work with Government Rather than Against It”, *MIT Technology Review*, June 2016, https://www.technologyreview.com/s/601489/why-tech-companies-should-work-with-government-rather-than-against-it/.

90. Greenblatt, Nathan, “Self-Driving Cars Will Be Ready Before Our Laws Are”, *IEEE Spectrum*, 2016.

91. Ibid.

92. Ibid.

93. HM Government and Marsh, *UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk*, 2015.

94. Ibid.

95. US Department of Homeland Security, *Enhancing Resilience through Cyber Incident Data Sharing and Analysis*, 2015.

96. Ibid.

97. Ibid.

98. Press Information Bureau, Government of India, Vice-President’s Secretariat, *Adoption of global standards will improve our productivity: Vice President Delivers Dr. M. Visvesvaraya Memorial lecture on ‘Enhancing Indian Productivity: Role of Global Standards’*, 2016.

99. Ibid.

100. Ibid.

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744

contact@weforum.org
www.weforum.org