StrategicRISK

SPECIAL REPORT:

BUSINESS TRANSFORMATION

The Fourth Industrial Revolution is upon us, bringing a whole new world of technology. The likes of AI, quantum computing and virtual reality are no longer science fiction and the threats associated must be on your risk radar.

In association with

AIG

Conquer the great 4IR tech wave

The Fourth Industrial Revolution is bringing a swell of advanced technology set to transform our risk landscape. The message is clear – move fast and smart, or risk going under.

Systemic leaps rather than a smooth line of gradual development have always defined human progress. These have often taken the form of industrial revolutions, which have seen rural societies become industrial, the implementation of mass production, and digital capabilities being brought to billions.

However, the latest version of these shifts might be the most distinct, rapidly spiralling and risk-filled one ever experienced – the Fourth Industrial Revolution (or 4IR).

According to Klaus Schwab, founder and executive chairman of the World Economic Forum, the 4IR is characterised by "a range of new technologies that

EXPERT VIEW: RISKS AND REWARDS OF A DIGITAL REVOLUTION

Advancing tech is set to bring us more information and capabilities than ever before. But, says AIG's Sheri Wilbanks, with great data comes greater liability. We must come together to face this new world of risks.

Technology advancements are transforming business in a big way. The past few years have seen the development of highly intelligent, automated and super-efficient solutions, which are reinventing how companies in all industries and markets are doing business. Some are calling this global trend the Fourth Industrial Revolution .

The IoT is at the forefront of this revolution. Organisations are embedding IoT into their operational processes, products and service platforms. Combined with AI, traditional machinery like automobiles, are applying AI subsets, machine learning and reinforcement learning, to enable autonomous driving.

Virtual reality (VR), while still in its infancy, is set to augment learning and development for the tasks that intelligent computer systems cannot replace. Combining this technology with data on environments, scenarios and outcomes, VR creates simulated environments, placing individuals in 'real-life' situations, where they learn by interacting with the 'environment', rather than simply analysing it.

Advanced visualization tools include extended reality mediums like VR, augmented reality, and mixed reality. These can provide risk managers with greater insight and understanding of their supply chains and more incisive risk assessment of natural catastrophes, for example. Combining IoT, AI and super computing thereby offers a plethora of new opportunities for risk management. They are not, however, without their challenges.

"COMBINING IOT, AI AND SUPER COMPUTING OFFERS A PLETHORA OF NEW OPPORTUNITIES FOR RISK MANAGEMENT. BUT THEY ARE NOT WITHOUT THEIR CHALLENGES."

Global innovation lead, AIG Client Risk Solutions
Sheri Wilbanks

LIABILITY RISKS: KNOWING TOO MUCH?

IoT adoption generates huge volumes of data on just about anything and everything that can be connected, running the risk of information overload. The challenge for risk managers is in extracting meaningful and actionable information from a sea of seemingly unstructured data. There is also the potential of new liability issues.

Take an example of a connected piece of manufacturing machinery. If IoT sensor information identifies the developing potential for an issue to occur, would the manufacturer incur legal liability for failing to act upon it or notify the user?

Similar questions arise when it comes to wearable technology. Sensors on these devices have the capability of indicating a potential or future health or safety issue. Like the machinery example, if an employer fails to act or notify the individual, they too could be potentially liable.

Liability challenges also exist with AI. Through algorithms, these technologies change as they begin to recognise and categorise items. As it continues machine-learning, the technology will, over time, evolve and act differently to the technology that you started with. The tricky question is, in an event of a loss, who is liable: the user whose 'behaviour' trained the algorithm or the manufacturer?

THE INSURER'S RESPONSE

Insurers are front and centre in recognising the opportunities and challenges associated with these technologies, keeping a pulse on how they evolve and their impact on the risk landscape.

We are also coming together as a community to share our learning and to help companies understand the risks and the risk transfer and mitigation solutions available. At AIG, we are at the forefront of testing these new technologies, learning both about the successes and the failures. This helps us in creating risk transfer and mitigation solutions that are fit for the future.

are fusing the physical, digital and biological worlds, impacting all disciplines, economies and industries, and even challenging ideas about what it means to be human".

The 4IR has heralded a new wave of advanced and highly intelligent automated technologies that augment human workers, optimising efficiency and productivity while cutting down costs. This includes 3D printing, the Internet of Things (IoT), artificial intelligence (AI) and drones.

These developments are intensifying traditional risks, bringing in entirely new risks and, ultimately, transforming the risk landscape for corporates.

According to the World Economic Forum's The Global Risks Report 2017, as different infrastructure networks become more interdependent during the 4IR, there is growing scope for systemic failures to cascade across networks, affecting society in multiple ways.

The report states: "Systemic risks can come from many directions – whether these are cyber attacks or software glitches, solar storms or even just unexpectedly

widespread and persistent clouds – and the increased complexity brought about by the 4IR makes the severity of those risks very difficult to estimate."

DISRUPTERS ARE EVERYWHERE

So how exactly is the 4IR impacting the severity and regularity of risks for corporates? And which risks are becoming more prominent?

"The answer to that depends on which industry you are thinking about," says Eamonn Cunningham, former chief risk officer at Scentre Group. "The risks that are emerging will impact all businesses, with some subject to potentially acute consequences. The backdrop to the Fourth Industrial Revolution is a business environment that is increasingly complex and challenging. Systems are more likely to be interconnected."

Cunningham says there will invariably be hyper competition and whether a firm is big or small the message is the same – innovate or perish.

"Disrupters are everywhere. The impact of this environment on certain traditional risks is also exaggerated. For example, with supply chain lines increasingly dependant on constantly functioning systems, it takes very little interruption in systems to have immediate and severe knock-on effects on those stretched and fragile production supply lines. You no longer have the comfort of a cushy time buffer – everything is 'now'."

Franck Baron, group general manager, risk management and insurance at International SOS, observes that when it comes to the 4IR, he is seeing an acceleration of changes in the medical and travel security services firm's risk maps.

"The 4IR is creating a higher level of uncertainty in assessment of certain risks, both in terms of severity and regularity. It is like witnessing the creation of a new norm or paradigm, a real shift in terms of how risks appear, mature and compare with each other. Risks related to cyber, digital agenda, innovations, technologies, market positioning and reputation are becoming more and more critical," he says.

Cunningham specifically points out that AI is an area where views vary on the impact it will have. "While efficiencies will arise in manufacturing, production and the provision of services, many see a people risk in the form of perceived job losses.

"This could simply be a repeat of those fears from 40 years ago that computers would take over some jobs, as this had yet to be played out. What is emerging is the anxiety driven by this fear. My own feeling is that this will instead create a demand for labour in areas that we just cannot envision today," he says.

WHAT DO WE HAVE TO FEAR?

There are a number of specific risk pressure points for the 4IR. Even if we truly understand the technology, the risks it will create are even more difficult to factor.

"IT IS LIKE WITNESSING THE CREATION OF A NEW NORM OR PARADIGM, A REAL SHIFT IN TERMS OF HOW RISKS APPEAR, MATURE AND COMPARE WITH EACH OTHER."

Group general manager, risk management and insurance, International SOS
Franck Baron

3D printing has already consumed some awe-inducing column inches for what it can achieve, especially around charitable and humanitarian causes, such as printing limbs for amputees or tools in developing countries. However, there is a risk-filled side to the 3D printing coin. For example, it could spark a glut of counterfeiting or make gun control more difficult.

And while AI promises automation that can fuel new levels of productivity, it could also result in weaponisation and spark a geopolitical crisis. Cyber attacks could escalate into industrial or political espionage. Autonomous vehicles create moral dilemmas, such as how they should act in certain accident scenarios – who should they kill and who should they save?

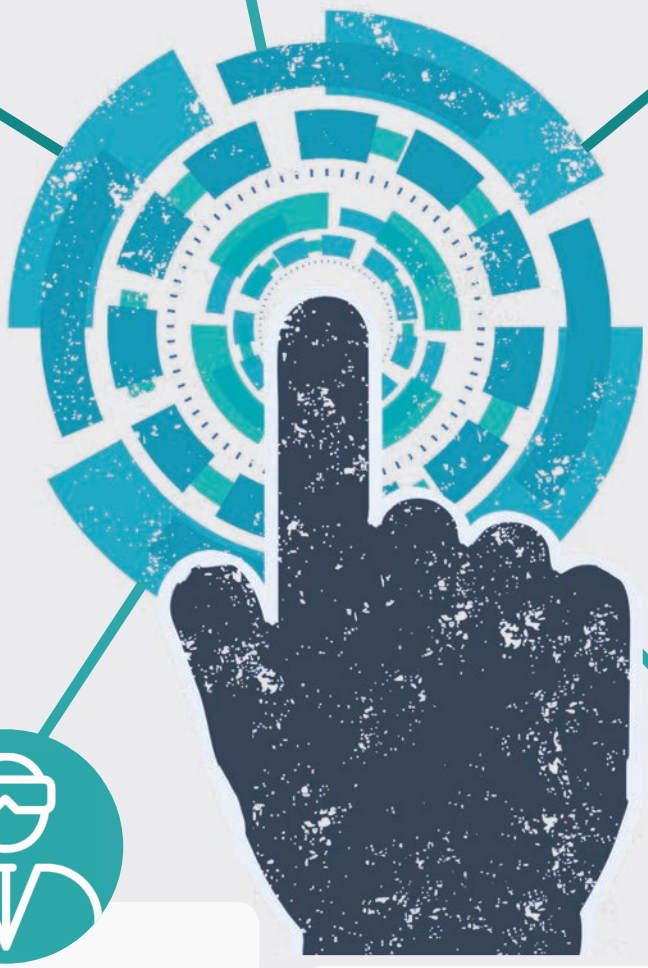
All this takes place alongside the traditional technology fear that 'the robots will be taking our jobs' and questions over the future of the traditional workforce.

"The Fourth Industrial Revolution is quite different to it predecessors in that changes are occurring at an increasing rate," says Cunningham. "Today you must consider not only traditional likelihood and consequence, but also the velocity of these risks when finalising those risk assessments. If you do not have regard to this, then your resultant risk mitigation strategy will not be perfectly calibrated and unexpected outcomes will arise."

Baron says at International SOS it is about ensuring the right level of technology monitoring, investment and concrete applications that can provide a better experience to its members and clients. "The risk then is linked to our capacity to do so and ensure a relevant level of focus and investments."

Whichever form the risks of the 4IR take, risk managers will need to be informed, nibble and progressive to sure its benefits are harnessed while its pitfalls are avoided.

Top five tech disrupters



INTERNET OF THINGS
What The connectivity of an array of devices, vehicles and home appliances.
Worry IoT raises risk concerns over the increased complexity it will create for networks and the new privacy concerns as data spreads wider than ever before. Risk management tools may be insufficient, with a lack of a global standard for IoT. Resulting costs could include reputational damage if personal data is hacked and upgrade costs to prepare the correct risk management tools.

ARTIFICIAL INTELLIGENCE
What AI simulates human intelligence processes in machines and computer systems.
Worry Risks include the weaponisation of AI by criminal groups or governments. AI could bring mass automation, meaning job losses. There could also be a skills gap in finding people to manage the AI systems. Risk managers can expect cybersecurity budgets to rocket as a result.

3D PRINTING
What The ability to solidify materials into a three-dimensional object.
Worry It brings counterfeit product concerns, alongside guns and weapons capabilities, and national security risks over the difficulty of tracking production. Firms could lose money through the loss of IP in counterfeiting or paying for additional 3D print security measures.

AUGMENTED REALITY
What The technology that superimposes a computer-generated image on a user's view of the real world.
Worry There are privacy concerns over which images are used, while the immersive nature of the experience could even have psychological impacts on users. There could also be unexpected legal costs in an area with almost no case history.

DRONES
What Unmanned aircraft flown using a remote control.
Worry Drones often have cameras attached so create privacy issues when flown over private property. They can also interfere with planes, be hacked themselves and could be used for smuggling. Potential costs could include compensation for those impacted by drones and training expenses if staff use them.

Disrupters on the horizon

Two great tech advancements – artificial intelligence and quantum computing – bring both potential threat and opportunity. Whether or not you believe you should act now or wait, keeping a watchful eye is critical.

Artificial intelligence is a tech disruptor that is already promising much. It can supercharge medical research, reduce human error on roads and at work, and fuel productivity in businesses across the world.

But these progresses are not without collateral damage for the risk community, where hacking, cyber crime and data theft can all be expected to arrive in fresh and surprising forms.

And not far into the horizon is the next great tech disruptor – quantum computing, which could further intensify the risks. It may be another decade before the business world is introduced to scalable quantum computers, but turning a blind eye to this emerging and high-impact disrupter would be a serious mistake.

So what are the biggest risks and opportunities for businesses around AI? And how will quantum computing then escalate these risks further?

DON'T TAKE YOUR EYES OFF AI

"AI is already impacting risk management, both as a threat and an opportunity," says Andrew Potter, general manager, risk and compliance, at tech-focused BAI Communications.

"Companies need to assess if they should adopt AI now or simply sit back and follow the trend of late adoption, and if this will cost them a competitive advantage. What is the impact on strategic goals and objectives and where are the new opportunities and threats? One thing is certain – get it wrong and it is unlikely you will get a chance to recover."

"ADVANCEMENTS IN COGNITIVE MODELLING, ROBOTICS, MACHINE LEARNING AND DEEP LEARNING ARE PAVING THE WAY FOR RISK MANAGEMENT TO PLAY A MORE STRATEGIC ROLE IN THE BUSINESS."

Deputy head of advisory, KPMG
Irving Potter

Chris Corless, who has held several risk management leadership roles at the likes of Vale, BHP, South32 and Orica, says he sees several upsides when it comes to AI in risk management, especially with operational risks.

"AI will be instrumental in helping us to identify data sets and triggers that will help to automate control effectiveness monitoring," he says.

"As for the risks associated with AI technology, that's a bit tougher to see. While AI will likely be able to help us solve some of the greatest problems facing humanity, such as climate change for example, there could well be unintended consequences if we create a new sentient being with greater cognitive capability than all of humanity combined."

AKTUS principal consultant Hans Læssøe believes AI will have a profound impact on risk management in a number of ways, including risk data being more precise and faster to obtain – and it will enable decision makers to make more precise decisions faster than they could do so before.

"While AI will help to reduce the level of uncertainty, it may be matched by an increase in uncertainty driven by the greater speed of change, competition and globalisation," he says.

AI is transforming the entire way that risk management is viewed and performed, says Irving Low, partner and deputy head of advisory, KPMG in Singapore. "Significant advancements in cognitive modelling, robotics, machine learning and deep learning are paving the way for risk management to play a more strategic role in the business."

"While AI is disrupting operating and business models, including transferring routine analytics and monitoring to technological solutions, it is enabling the risk function to support the business in achieving efficiencies, such as receiving high-quality analysis to support business decisions faster."

TAKE QUANTUM COMPUTING SERIOUSLY

BAI Communications' Potter acknowledges that quantum computing is theoretical at this stage but believes it is not improbable in the next decade.

"That does not mean it should not be considered seriously now," he adds. "If we learned anything from 'Y2K', it's that this tech needs to be debated from a risk perspective – you could end up making a significant financial investment for an event that essentially does not eventuate."

Potter explained that if the risk threat of quantum computing does materialise, it will have a significant impact on the security of an organisation's data. "Organisations like Facebook and Google have a lot to fear and potentially huge expenses to protect against the threats such a risk would pose. And it is not just about data loss but also safety – imagine if airlines were compromised during flight, or utilities or even hospitals were brought down."

Neil Allan, MD of Systemic Consult and partner at RiskIQ, says: "The way quantum computing works – with qubits and 'multiple states' active at the same time — is highly complex. While it's not yet all-pervasive, quantum computing will have an increasingly large impact on society in the coming years. Quantum computing will undoubtedly have many positives but, as always, there are risks to consider."

"IF WE LEARNED ANYTHING FROM 'Y2K', IT'S THAT THIS TECH NEEDS TO BE DEBATED FROM A RISK PERSPECTIVE – YOU COULD MAKE A SIGNIFICANT FINANCIAL INVESTMENT FOR AN EVENT THAT DOES NOT EVENTUATE."

General manager, risk and compliance, BAI Communications
Andrew Potter

A THREAT TO MODERN ENCRYPTION

If quantum computing could defeat all modern encryption, this could have implications for cybersecurity. Potter says: "Quantum computing has the potential to significantly disrupt the cybersecurity environments we have today, leading to company and personal information being exposed at a speed and mass beyond anyone's expectations."

"Senior management, C-suite and boards in all industries will need to comprehend the consequences that quantum computing will have on their legacy systems and identify measures and controls to be prepared."

Daryl Pereira, partner and head of cybersecurity, KPMG in Singapore, states that quantum computers will reduce the time needed to solve complex mathematical problems used in encryption.

"Eventually quantum computing will reach a level of maturity to pose a threat, but steps are being taken now by governments and cyber research organisations to publish stronger approaches that directly address post-quantum computing cryptography," he says.

Overall, risk managers must continue to monitor the developments in AI and quantum computing to understand the future risk landscape, without getting ahead of themselves as the technologies continue to change and mature. The key for risk managers is to ensure their involvement in any forays into AI and quantum computing are at the very start of the process.


Insuring the impossible.
In an ever-changing world, AIG empowers clients to embrace every new opportunity. Discover personalized insurance solutions powered by the latest technology, innovative partnerships, and industry-leading experience.
AIG
Bring on tomorrow®
Insurance, products and services are written or provided by subsidiaries or affiliates of American International Group, Inc. Insurance and services may not be available in all jurisdictions, and coverage is subject to actual policy language. For additional information, please visit our website at www.AIG.com.