CNA / HARDY

Facing Up To The Fourth Industrial Revolution.

Dave Brosnan, CEO, CNA Hardy

This article first appeared in Insurance Insider's Quarterly publication – Spring 2019

Facing up to 4IR

This article first appeared in Insurance Insider's Quarterly publication – Spring 2019

The Fourth Industrial Revolution which focuses on advances in communication and connectivity is the insurance industry's greatest test yet.

It took centre stage at the World Economic Forum annual meeting in Davos this year, with session after session agonising over its impact on the global economy and geopolitics.

Our own research underpins the extent to which company activity is driving the progress of the Fourth Industrial Revolution – blurring the boundaries between the physical and digital, company and government, national and international.

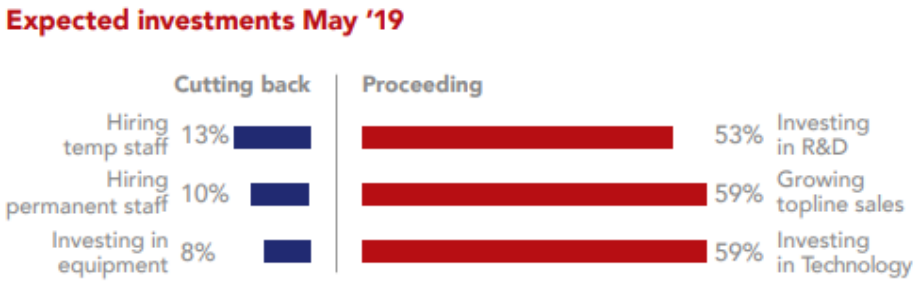
It also suggests the Fourth Industrial Revolution will prove the biggest test yet for insurer-business relationships as we grapple with the challenge of ever-greater technology integration and global interconnected risk.

Tech commitment

Simply put, the Fourth Industrial Revolution refers to how technologies like artificial intelligence, autonomous vehicles and the Internet of Things are transforming how businesses function and how people work.

Even the most basic tasks – a farmer planting a crop, a manufacturer ordering parts, a patient taking a breath, or a customer paying a bill – can be monitored, supported or even supplanted by technology in the room, through the Cloud, or on a server on the other side of the world.

Our research shows that technology is an increasingly critical area of spend for companies seeking to drive efficiency, profitability, innovation and closer customer interaction. Three quarters of business leaders we spoke to across the world in November 2018 for our Risk and Confidence report 'Global Risk and Confidence Survey are prioritising technology spend over all other.



Indeed, in the digital age, it is the technology and research and development spend where businesses are choosing to concentrate their firepower, rather than on technology and talent, as was the pattern two years ago when we first began our business risk and confidence research.

As companies cut back investment on both hiring temporary and permanent staff, and on corporate development such as M&A, the trend is all too clear – companies are confident and preparing for growth, but are also looking to technology to give them that all important 'edge' by improving service and making their businesses more efficient and effective. The result will be a tidal wave of further innovation and disruption to everyday life and a shift in the way we prepare, mitigate and manage risk.

Tech risk concern

However, the recent agonising at Davos demonstrates that technology is not an unmitigated force for good. While, on the one hand, technology offers businesses a range of fantastic opportunities as the interconnectivity of machines, systems and processes increases, it also brings questions around security, data protection, business continuity and third-party liability, as well as containing the potential for critical infrastructure breakdown.

We define tech risk in our research as the danger of making the wrong investment decision, or of allowing technology assets to age, making the business inefficient or uncompetitive.

The UK banking sector is a prime example of tech risk in action. Despite investing billions to overhaul outdated and overloaded IT systems, high street lenders suffered a string of outages in 2018, most notably at TSB but also at Barclays, RBS and HSBC. Customers were left unable to withdraw cash, access apps or pay their staff.

The experience of the UK banking sector in 2018 was a lesson, if one were needed, on the severity of tech risk and how it can lead to less obvious, but equally severe, interconnected risks.

As a result of the TSB failure, the UK House of Commons announced a public enquiry, the UK Financial Conduct Authority and Information Commissioner's Office launched regulatory investigations, and there was widespread loss of consumer confidence and significant reputational damage.

Interconnected risk

In our Risk and Confidence surveys undertaken since 2017, business leaders consistently fail to understand the new equation heralded by the Fourth Industrial Revolution – namely that a tech-enabled integrated world creates a web of interconnected risk.

In our surveys, for example, business leaders persistently under-rate the significance of the interconnected regulatory and reputation risks that flow from a cyber-attack or technology failure.

- In 2018, only 13 percent of respondents ranked regulatory and compliance risk top, and a mere 6 percent were most concerned by reputation risk.
- Looking ahead to 2019, less than a third of company leaders thought reputation risk would rise and less than half thought regulatory and compliance risks would increase.
- Supply-chain risk likewise languishes at the bottom of the risk league table, despite Maersk being shut down for 10 days back in 2017 following the NotPetya malware attack.

The inexorable increase in connected devices, with the Internet of Things, the digitisation of supply chains, and more widespread adoption of AI in industries from medical diagnostics to electricity demand management, can only expand the number of fronts that criminals and nation states can exploit.

In a sad indictment of human failure to translate information into action, more than three quarters of the companies expect to become a target of a cyber-attack, yet only 23 percent comply with minimal cyber security guidance or regulations, according to cyber security firm Kaspersky ('The State of Industrial Cybersecurity 2018', June 2018).

Reassessing risk management

The reality of interconnected risks means insurers, brokers and risk managers will need to work ever more closely to build appropriate resilience into business systems, processes and assets if we are to navigate the Fourth Industrial Revolution successfully. In particular, we need to explore how we can leverage technology more effectively as part of the fightback.

While technology can augment risk, it also brings the power to augment our own skills, and developments such as AI really can help hold back cyber-crime, especially the huge state sponsored attacks.

It is predicted that 2019 will see big growth in AI-on-AI cyber battles as we seek to harness technology to protect our digital assets, and this is positive all round.

New technologies are also boosting risk analysis. Insurers now use drones to analyse damage to crops and buildings following natural catastrophes in territories across Africa, the US and Europe. Some are deploying semantics analysis to better understand supply chain risk, or partnering with InsurTechs to identify next generation litigation risks.

In an increasingly networked world, data from devices known as the industrial Internet of Things in factories and supply chains will provide an opportunity for even better risk assessment through predictive indicators and more flexible, tailored and timely solutions.

Cameras, for example, can monitor machine tools 24/7 and report immediately when tolerances are exceeded. Likewise, automated sensors can track every stage of the storage and shipment of temperature controlled pharmaceuticals, ensuring that manufacturers and logistics providers can monitor risks and prevent losses before they occur.

In a technology-driven, integrated world, the aim must be to understand and manage interconnected risks more quickly and prevent losses before they occur.

It might not make Davos meetings more upbeat, but it will help ensure that insurer-broker-insured relationships are more productive – and that we develop products that manage these complex risks more effectively.

By Dave Brosnan,
CEO,
CNA Hardy

Further Reading:

CNA Hardy Risk & Confidence Survey Nov'18 edition

CNA Hardy Future Insight Report: Technology