Sponsored by

CIR
CONTINUITY INSURANCE & RISK
thinking resilience

AXA Corporate Solutions UK's Client Forum examined the opportunities and implications of the digital explosion. From cyber security to insurance and wargaming, what should risk managers be doing to both protect and profit from data?

Data: Panacea or placebo?

Sponsored by


Corporate Solutions
It pays to think ahead
At your side helping you conduct your business, today and in the future. Whatever happens, wherever your business takes you.

Panacea or placebo?

AXA Corporate Solutions UK's Client Forum examined the opportunities and implications of the digital explosion. From cyber security to insurance and wargaming, what should risk managers be doing to both protect and profit from data?

Data has become the lifeblood of business, with big data promising enormous opportunities but at the same raising significant issues. The risk and insurance implications are numerous, complex and fascinating all at once; benefiting from the data explosion requires a considerable change of mindset amongst all industry stakeholders.

"With the consolidation of all the information we create every day, we can begin to see previously hidden relationships and make unprecedented predictions. We can use this in ways that even a few years ago were not possible, or even imaginable," enthuses Paul Lowin, acting CEO of AXA Corporate Solutions.

There are a number of obstacles to success, however. Data can be easily misinterpreted, and data privacy and security are growing issues – with cyber breaches hitting both headlines and bottom lines everywhere. No company is immune – eBay, Sony, TalkTalk, Yahoo and even the NHS – cyber attacks hit a staggering half of businesses last year. Meanwhile, will regulation make leveraging data just too difficult? And do we even have the skills to do all that we need to?

There is a lot to talk about. A sensible start would be to properly analyse the data we have to begin with. As Chief Underwriting Officer at AXA Corporate Solutions UK, Mark Platten, puts it: "If we all ensure we can trust the data we have, it will enable better conversations, which in turn lead to better decisions."

A data explosion

Understanding the scale of the data explosion and what it means for business requires a look at some vital, but simple statistics. Over 90 per cent of the data in the world today has been created in the last two years alone. Global Chief Operating Officer of AXA Corporate Solutions, Steven Haasz, frames it thus: "In terms of the 5,100 year history of data and data storage this means 90 per cent of the data in 0.04 per cent of the time."

The enormity of this data and technology explosion is difficult to visualise and we are adding to it all the time – creating a huge amount of additional data every minute of every day. By April 2017, some 3.8 billion of us were creating and consuming data, with more devices creating and consuming it. It is predicted that PC generated IP traffic will grow 10 per cent CAGR; smartphone IP traffic 49 per cent; and Machine to Machine (M2M) modules 49 per cent.

Haasz says that by 2021, there will be 27.1 billion networked devices, with machine to machine modules driving a large amount of traffic.

This is just four years away.

Physicist Stephen Hawking has famously warned on the dangers of unmanaged artificial intelligence, saying the emergence of artificial intelligence could be the "worst event in the history of our civilisation" and urging creators of AI to "employ best practice and effective management". It is an extreme scenario, but represents a timely warning.

Tech industry analysts correctly predicted the banking sector rolling out automating processes, using AI and robotic process automation (RPA) tools this year. And the insurance industry needs to catch up, or, as Airmic technical director and deputy CEO, Julia Graham, puts it "the banking industry is going to have its lunch".

The immediate priority rests first, however, with the security of data and systems. It was reported in October, one year since the National Security Strategy was launched, that in the 12 months leading up to that date, the National Cyber Security Centre responded to over 590 significant cyber incidents, more than 30 of which were sufficiently serious to require a cross-government response. A UK government official said that the Wannacry virus and recent attack on the UK and Scottish Parliaments could have been considerably worse had the NCSC and the NCA's National Cyber Crime Unit not been operational and in a position to lead the response.

The UK government's 2017 Cyber Security Breaches Survey showed that seven in ten large businesses identified a breach or attack, with the average cost to large businesses of all breaches in the year to July 2017 being £20,000 and in some cases reaching millions.

But in spite of a growing recognition of the value of technology and data assets relative to historical

tangible assets, only 15 per cent of probable maximum loss (PML) in EMEA is covered by insurance. According to Aon's EMEA Cyber Risk Transfer Comparison Report, some 38 per cent of EMEA businesses have suffered a cyber related loss in the last 24 months, averaging US$3.3m per loss; and yet they still spend four times more on protecting physical risks than they do on information assets.

There is much for risk managers to consider when it comes to the security of data, among the most pressing arguably being the upcoming General Data Protection Regulation.

GDPR: Need to know

The General Data Protection Regulation comes into force in May 2018. The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

The GDPR gives regulators considerably enhanced powers. If an organisation cannot demonstrate that good data protection is a cornerstone

"Insurers and brokers will mainly have GDPR issues with data retention and consent. Obtaining consent from the data subject in the first place can be really tricky"

of their business policy and practices, they could be leaving themselves open to enforcement action that can damage their reputation and their financial bottom line. Swift action will also be critical in the event of a data problem since the GDPR introduces for the first time a mandatory breach response regime. Businesses have just 72 hours from the time they discover a security breach, to assess if there is any risk to individuals and notify the Information Commissioner's Office. They must also notify the data subjects at the same time or shortly afterwards, if there is a high risk of harm to those individuals.

Stressing the power of fines under the new rules, Joanne Howie, Deputy General Counsel at AXA Corporate Solutions speculates that under GDPR, the recent TalkTalk incident would have cost the company some £59m.

"All contracts will need to be reviewed [to prepare for GDPR]. And this process should have been started already. Insurers and brokers will mainly have issues with data retention and consent. Obtaining consent from the data subject in the first place can be really tricky," she warns.

As Howie rightly stresses, time is of the essence when it comes to GDPR, with mere months to get your houses in order.

"Boards are not aware as they

should be," comments Airmic's Graham. "I think it will make business very careful about not just managing the data that they've got but what they will keep collecting. Ultimately it will make boards more conscious of where the crown jewels are. "If you ever want to wake your board up, this is the way to get their attention."

Asked what the insurance response to GDPR might be, Graham says it depends what happens as a result of the breaches. "Some of those risks are not only going to turn into loss of income, for instance."

Separating fact from fiction

With the sheer number of cyber attacks reported, it is easy to see why the risk has shot up the corporate agenda. The picture often looks quite bleak – the risk seemingly insurmountable, but it is vital that organisations get hold of it. In order to do that, the very unique risk picture for each organisation needs to be drawn up, addressed and reviewed regularly. Understanding exactly what the cyber threat landscape really looks like is a good point to start.

One individual who knows a lot about this arena is former UK government cyber security specialist, Jim Wheeler. His experience has seen him work in counter terrorism and counter cyber espionage operations and now in the private sector has seen highly sophisticated techniques used by cyber crime gangs and organised crime. Now CEO of ReSolve Cyber, Wheeler says we need to take a realistic approach to managing cyber risk. "Sadly, we know that nothing can be 100 per cent secure forever, as capabilities continually evolve. But, to reduce your risk from cyber crime businesses need investment in three areas: technology, process and people. It all starts in the boardroom; if the executive board do not understand the risks, how can the business mitigate against them? Most boards now need briefing on the cyber threat to be aware and to stay informed."

Speaking at AXA's Client Forum, Wheeler reiterated the warning over the extent of the social engineering threat, which, along with phishing, malware and ransomware, all individuals and companies are increasingly vulnerable. He says this exploitation of human kindness, trust and the untrained will continue to pose a threat, and that organisations must find a way to get to grips with it.

There is more change on the horizon when it comes to the human element. While Generations X and Y can generally be said to value privacy more than the younger Millennials, Wheeler expects to see a shift in attitudes, with a growing emphasis among this group on the importance of safeguarding their data.

"Privacy will be the big word," Wheeler predicts. "Things will change when younger people start to realise how important it really is to them."

This may turn out to be bad timing if a trend currently apace in China gains traction elsewhere. The country's Social Credit System, which sees points earned by citizens from such factors as credit history, fulfilment capacity, behaviour and preferences and interpersonal relationships, is currently voluntary, but will be mandatory in 2020. It is no great leap to imagine such a system being adopted elsewhere.

Combating these wide-ranging threat actors requires a truly joined up approach. "It's hugely important that you have all parts of the organisation involved in the approach to tackle cyber risk," says Scott Sayce, Global Chief Underwriting Officer of Cyber at AXA. "And this has to be

a continuous process." He points to the essential considerations for cyber security and information governance.

The first is company-wide buy-in, which should include board level strategy, training and education and at the individual level should seek to assign personal responsibility. This is vital to ensure best practice. Understanding that every organisation has unique vulnerabilities and needs a clear strategic vision is also key here. The next is resource; cyber security protection is now an essential budget line and is likely to increase as more sophisticated threats become commonplace. For organisations to have a clear view of the risks facing them, they must budget realistically. Thirdly, having the right knowledge can sometimes make all the difference; that means larger corporations with complex IT systems may sometimes need to seek external advice. Finally, expert controls will mitigate many of the vulnerabilities that may attract the wrong attention. Part of this means staff training, dedicated policies and of course regular assessments.

With that in mind, Sayce predicts a change on the horizon when it comes to dealing with the threat, emphasising that cyber wargaming will become much more needed and a staple part of crisis response and disaster recovery planning.

Where innovation lives

With so much of the discussion around cyber focused on the downsides, it is easy to forget the great many opportunities that come about if the risk is properly managed – for businesses of all size

Business Development Manager at AXA Corporate Solutions UK, Matt Reeves, is enthusiastic about the way a number of well known brands are already using big data.

"We see it in action in mainstream companies on a daily basis. Uber has no cars, Airbnb no hotels, and eBay no products, but they do have data."

Amazon is another such innovator. It has leveraged face recognition technology to underpin its Amazon Go model. The technology giant has just opened its first Amazon Go store in Seattle, and can predict customer habits with great accuracy. The company's Prime Air concept, meanwhile, poses a number of questions when it comes to logistics, but drone technology in mainstream applications is still in its infancy and even Amazon may have some way to go before this can be rolled out at any scale.

The insurance market is a notoriously traditional one, with much work still carried out face-to-face and reliant on strong business relationships. Will the rise of the digital age bring about the end to this tradition of the personal relationship in insurance? Can we not conduct all business by electronic communication from here on in? Do we really need to meet? The general consensus at the AXA Client Forum is that digital avenues should provide us with an opportunity to spend our time more wisely, and that there is no substitute for the value that relationships can create. As Aon Risk Solution's Guy Malyon observes: "While you may be able to analyse data to a certain degree, there are a lot of facts that may not always be captured." And those may indeed turn out to be the most salient.

"If you look at why you have won certain business over the years, it is based on trust and the knowledge that you can get on and do business together," Malyon adds.

Digital is changing the insurance market in other ways, and perhaps more slowly, but certainly surely.

" I don't think we have seen anything yet. We are heading for the unconventional at a rapid speed"

"I think in the digital future, there are going to be people dealing in a very different way with personal decisions and how they use data and how they relate to people," says Airmic's Graham.

"In insurance, we will start seeing the underwriter taking more information from the cloud. The days of asking for proposal forms and applications are numbered. Despite all this, you still need the relationship to decide what you're going to do with it. Do you believe what you see? I don't think we have seen anything yet. We are heading for the unconventional at a rapid speed."

The challenge will be understanding new mindsets and thinking about the possibilities from this new base. As the keynote speaker at the AXA Client Forum, statistician Christian Howes correctly observes, "data is definitely here, it's definitely now" and it is has already begun to have a significant impact on the way business is conducted in insurance, with much more change ahead.

Better decision making and analysis needs to be the central focus of all these efforts, with an open mind about the impact that may have on the industry and the subsequent need to be able to adapt with it. As Lowin notes: "Risk managers will be able to predict losses with increasing accuracy. All of you will know how much, how many and when and where losses will happen, so why transfer the risk? After all, it's not then a risk; it is a certainty. As insurers we need to transform to the point where we use the data we hold to partner risk managers and brokers."