Commercial feature

From payer to partner: transforming the insurance promise

What will the truly transformed insurer of the future look like? That was the question posed to industry experts during a roundtable exploring the technological, cultural, structural and ethical challenges facing insurers

Morag Cuddeford-Jones

Before tackling how transformation should occur, it's vitally important to understand why transformation is needed. According to Roland Scharrer, group chief data and emerging technology officer, AXA, it's because the fundamental relationship between insurer and insured is changing. "You're building a partnership with the client and you shouldn't be seen just once a year." This is part of AXA's 'from payer to partner' strategy.

"The more consumers invest in their connected devices – cars, homes, watches – you're building a partnership with them," adds James Barnard, CIO, Aviva tech shared services and divestments. "Everywhere they go, you're going with them. You're acting like a guardian angel."

There's no doubt that there is certainly much more opportunity through digital transformation to play a bigger role in consumers' lives – increasing engagement and, ultimately, ROI. But it's also a place to tread lightly. "It's important to be led by what the customer wants and where we think we can add value to the process," warns Anita Fernqvist, UK chief data officer and director of operations, Zurich Insurance. She notes that not every step of every insurance relationship needs the 'white glove' treatment. Simple, automated efficiency can add value too.

"That interaction point could be touchless, it could be automated, it could be empathetic – it could be all three," reveals Chirag Jindal, head of insurance, Americas, ServiceNow. "Insurance is a promise and we have to wrap the narrative of the customer journey with that promise in mind. But how you wrap that around technology to deliver it and let the customer choose – that's the problem we are trying to solve." And, he adds, "we have to be cohesive".

Here is the biggest challenge insurers face. The customer has expectations, set not by other insurers but by the likes of Netflix, Amazon and ASOS. They expect the process to simply work. Getting that process to work end-to-end, whatever happens, is far from simple.

"You have a lot of expectations of an Amazon-like digital experience but insurance is a very complex product and you have to serve the client at very specific moments of truth," warns Scharrer. It's something that insurance companies may have been doing for centuries, but while that delivers a huge amount of experience, it also brings with it some significant hurdles.

"For an organisation like ours, the real challenge is updating our core infrastructure, cloud capability, robotics and intelligent automation to bridge what is expected of us by consumers today," Barnard reveals. Being constantly available, leveraging digital currency and providing a seamless transition into what can, quite often, be 70-plus years of legacy estate."

So that cohesiveness that Jindal speaks of begins to seem like a pipe dream, given the scale of the challenge. The challenge of bringing a sprawling, global insurer with decades of legacy systems and customer information into a seamless, end-to-end experience in a single, smooth action.

We have to add to this that the insured aren't just large organisations, they serve a massively diverse audience. "We have very different customer segments and that means one size does not fit all. We have to be really clear about what real-time really brings to customers, for example. In other places, [the importance could be] relationship-led [interactions] with digital interventions, rather than end-to-end," Fernqvist insists.

At times, it can seem that there are hurdles at every turn. Cloud transformation, for example, is seen as bringing major advances in insurers' ability to overcome legacy issues, but it too comes with its own set of challenges. "On the one hand, we need the cloud to provide the elasticity of infrastructure, scale and availability," says Scharrer, "and at the same time you must ensure a high level of data privacy standard." And still, he adds, transform the legacy environment.

How data is treated in the transformation piece is critical. As a heavily-regulated industry, one might argue that insurance actually has an advantage in the face of a data-sceptical public. Its trust is surely baked in as a result of those tightly defined parameters. Fernqvist concurs: "Trust is critical. For us to serve [our customers'] needs, we need their data. We've got to be able to handle it in such a way that we've earned and retain that trust. Regulation helps us protect our customers and make sure that we're building with the customer in mind."

Data governance is, therefore, a key concern and again, due to the often diffuse and complex nature of insurance organisations, not one that is easily managed. "The ethical use of data is very important. We have 18.5 million unique customers and that's a tremendous amount of data. The use of third-party enrichment has levelled up the playing field but with that comes more responsibility," suggests Barnard.

Scharrer adds that building a data-led or data-fed culture is critical. He says it's about bringing "a data-driven culture that's understood from the claims handler to business decision-makers. Bringing the whole organisation behind that, either through incentivisation or governance, so that it's protected and leveraged as an asset."

Of course, it can only be truly leveraged as an asset if the right people can access the right information at the right time. Organising where data is held and how it fits into the multifarious workflows can be a task of mind-boggling complexity, but Jindal has some suggestions which marry closely with how integrating new channels and technologies can work more effectively across the organisation as a whole.

"You need some kind of orchestration layer that can tie the broker experience to the middle and the back offices, and carry that across the value chain," he advises. "At every point of the journey, everyone should know what the status is. How you orchestrate that has been the biggest challenge that insurers are talking about." Specifically from a data organisation perspective, he adds: "How do you present the right data to the right person at the right time? You don't want to overwhelm them. What does a claims agent or customer service operative really need to look at?" Fernqvist agrees, stating: "One of the big challenges with data is figuring out what needs to be centralised but also how we make sure we decentralise to allow innovation."

Innovation in this context is key. The world is moving fast and insurers need to be able to make the most of the latest technologies – themselves highly dependent on quality data – to stay ahead of the game. Scharrer points out the use of AI to be able to ingest other data sources such as documents, photos and satellite technology to speed up and enrich customer interactions but warns about being too hasty and insists on the importance of data quality. "There has been an expectation that AI solves all our problems in databases and customer journeys. But people are realising it's still hard work."

Barnard is, however, undeterred: "Cognitive learning is a really powerful tool. That's where we start unlocking the value of rich data and that's come a long way in the last three years." This whole process, Barnard concludes, "is a really exciting journey that we've only just started."

> **At every point of the journey, everyone should know what the status is. How you orchestrate that has been the biggest challenge that insurers are talking about**

Panel

James Barnard, CIO, Aviva tech shared services and divestments

Anita Fernqvist, UK chief data officer and director of operations, Zurich Insurance

Chirag Jindal, head of insurance, Americas, ServiceNow

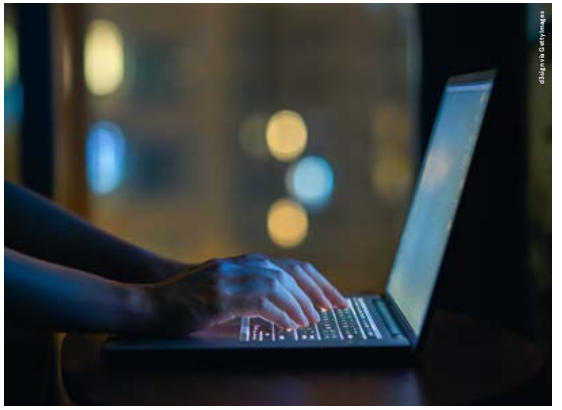
Roland Scharrer, group chief data and emerging technology officer, AXA

CYBERSECURITY

Is your company at risk from silent cyber?

With cyber attacks on the rise, companies must ensure they have the right insurance policies and business practices in place to safeguard themselves

Alex Wright



Technology is enabling businesses to grow further and faster than ever before, accelerated by the need to digitalise in the wake of the Covid-19 crisis. Despite the undoubted business benefits, this period of rapid change has also left companies more exposed to cyber threats than ever.

Many of these cyber risks are so new and complex that most firms aren't prepared for them. Worse still, in the event of a cyber attack, companies' traditional property insurance coverage won't protect them because many of these risks aren't implicitly included or excluded within the policy – a phenomenon known as 'silent cyber' or 'non-affirmative cyber'.

And businesses often only find out they're not covered when it's too late, as evidenced by the WannaCry, Petya and NotPetya cyber attacks of 2017, which devastated everything from shipping ports and supermarkets to advertising agencies and law firms. These attacks can be hugely damaging, not only operationally and financially, but also in terms of reputation. According to IBM's Cost of a Data Breach report 2021, organisations shell out, on average, $4.24m (£3.22m) per incident.

"As a risk, silent cyber still isn't on the radar of most organisations," says Tracie Grella, AIG's global head of cyber risk insurance. "The problem is that they aren't assessing the risk and working out where their exposures are, how their policies will respond and whether they would be covered for an event."

So what are the cyber risks companies need to be aware of and what should they do to mitigate against them? What insurance do they need to protect them if an attack occurs – and how can they plug any gaps?

The fastest growing and most costly form of cyber attack is ransomware. Often originating in nation-states such as Russia and its neighbouring countries, ransomware attacks use malicious software to block access to a computer system and the hacker will then typically demand large sums of money – often in the multi-million dollar region – for the system to be unlocked again.

Phishing or social engineering scams are on the rise too, with victims sustaining $1.7bn in losses from business email compromise alone in 2019, according to the FBI's Internet Crime Report. But the costs go far beyond the initial loss: they extend to business interruption, forensics, recovery and restoration expenses.

To guard against cyber attacks, businesses should try to prevent them from happening in the first place. That requires identifying their key exposure areas to cyber risk, quantifying loss scenarios and appetites, and establishing robust cybersecurity and risk management strategies and controls that everyone in the organisation understands.

> **When a client suffers an event, often there's a disconnect between what their policy actually covers them for and the appropriate coverage they would need**

Networks and systems should be regularly updated through the latest security software backups on the cloud, patches and upgrades, and tested to make sure they are protected. In addition, companies should restrict systems access only to those who need to use it, particularly when dealing with third-party providers. Firms should encrypt data, adopt virtual private networks and use multifactor authentication.

The key to improving cybersecurity is ensuring staff receive regular training so they can identify suspicious activity and potential problems. This includes not opening unsolicited emails, creating strong passwords and not using personal devices for work.

Should the worst happen, firms also need to have cast-iron incident response, disaster recovery and business interruption plans in place to get back on their feet quickly. Insurers can help both with designing a risk mitigation plan, and providing access to the necessary legal, forensic and claims teams needed post-event.

Insurance policies can help businesses recover their losses after a cyber attack. However, many companies that previously relied on their standard property or liability policies have now found – to their cost – that they're no longer covered.

"Cyber risk has implications across the board," said Rich Sheinis, data privacy and cybersecurity partner at law firm Hall Booth Smith. "When a client suffers an event, whether that be a ransomware attack or a business email compromise, often their policy isn't geared up to deal with the potential losses they will incur, and there's a disconnect between what their policy actually covers them for and the appropriate coverage they need."

A common problem is silent cyber, which means that potential cyber-related events or losses are not expressly covered or excluded within traditional policies. This can lead to unexpected coverage gaps.

There is a solution. Standalone cyber insurance protects companies specifically against cyber attacks, providing emergency incident response and recovery services, ransomware negotiation and reimbursement, business income loss and follow-on liability coverages.

They will help to plug coverage gaps, protecting against losses caused by damage or data loss from IT systems and networks. The policy can also be used to engage a PR firm for managing a cyber incident in the media when reputation is at stake.

If a business has more than one policy, it's vital to check there's no overlap or duplication of cyber coverage.

"In order to ensure the best outcome, it's imperative for businesses to work with a specialist cyber broker to review their coverage thoroughly to see what they need and be able to explain the risk fully to the underwriter," says Kyle Bryant, chief underwriting officer at Resilience.

"There are plenty of innovative solutions out there to meet any company's individual requirements and plug any gaps they may have."

ARE INSURERS TAKING CYBER SERIOUSLY ENOUGH?

Percentage of global insurers who say they expect to increase spending in the following areas in 2022

Deloitte, 2021