

# New Technologies in the insurance industry

Ty Yiu

2019-04-04

## Overview

Although insurers recognize the power of analytics to grow, optimize and protect value, many continue to be overwhelmed by the far-reaching changes required to transition to value-driven decision-making.

Ask yourself: What cultural and organizational changes are necessary to become data-driven and analytics-led? (*EY*, 2019)

Technologies worth considering: - Artificial Intelligence & Machine Learning - Deep Learning - Computer Vision - Analyse risks of a construction site, *on-site*, by having a machine learning computer vision model identify *dangerous* situations/circumstances, to classify risk. E.g. Camera detects a not-well secured construction site with overhanging, loose steel beams. The potential risk is different than in e.g. a coal-mine. - Natural Language Processing - Human Sentiment Analysis - *Strategies/Methods affected*: - Business Intelligence - Predictive Analysis - Operations optimisation (minimising deficiencies, maximising efficiency) - Prior Profiling Integration/Consideration - There are more records in existence than directly available to insurance firms (to use for a basis of risk classification), thus using AI to go through these staggering amounts of profiles, that exist on the web, and combining them into one, massive, detailed profile. - Behaviour Analysis - Online, offline[using computer vision via cameras, like Amazon is detecting behaviour patterns in their *GO-Supermarkets*] - Risk Analysis

- Based upon \*Behaviour Analysis, Sentiment Analysis & prior profiling integration)
- Blockchain
- Cyber-Security
- Distribution of responsibility/power
- Decentralisation
- Acceleration
- its faster and better

## Artificial Intelligence & Machine Learning

Artificial intelligence and Machine Learning for automated and self-optimising risk analysis / risk classification of (potential) customers/clients. The risk that a (potential) client of an insurance firm is exposed to, is vital to be identified, in order to adequately price the insurance. E.g. A construction worker on a sky-rise building is exposed to more potential risk than a construction worker that refurbishes the inside of an existing office building.

For those who are yet to embark on their journey towards AI in insurance, it is key to start investing in Artificial Intelligence now. For leaders looking to steer their organizational ships into the auspicious waters of AI and start investing in AI, the following guiding principles apply:

Assess the data at hand and accessible from the outside to get an initial idea of potential use cases, leveraging a bottom-up approach. Start small with applications on the lower spectrum of complexity and iteratively scale to more complex solutions as you grow your expertise. Don't be afraid of failure as AI applications are prone to various challenges and the key to success is to rather fail fast than to burn resources on non-promising projects. (*Deloitte* 2019)

### **INSURERS ARE FACING PRESSURE TO EVOLVE, AND VIEW AI AS A GAME-CHANGING TECHNOLOGY**

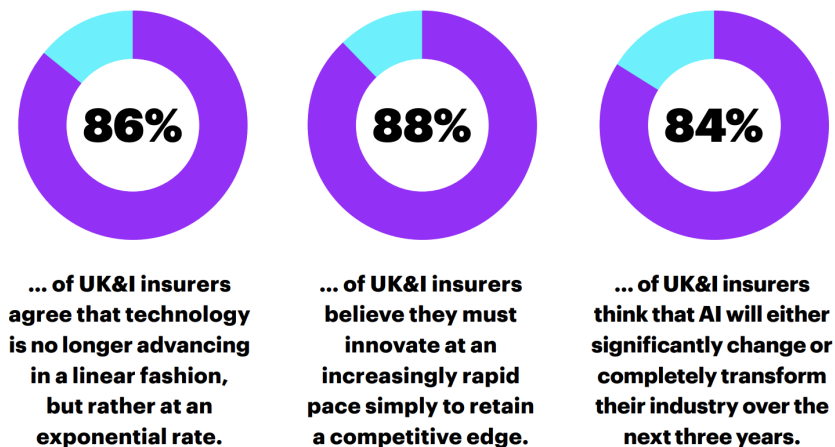


Figure 1: Data from Accenture's Technology Vision for Insurance 2017 (*Accenture*, 2019)

## THE MAJORITY OF CONSUMERS ARE READY TO EMBRACE VIRTUAL AGENTS AND ROBO-ADVISORS

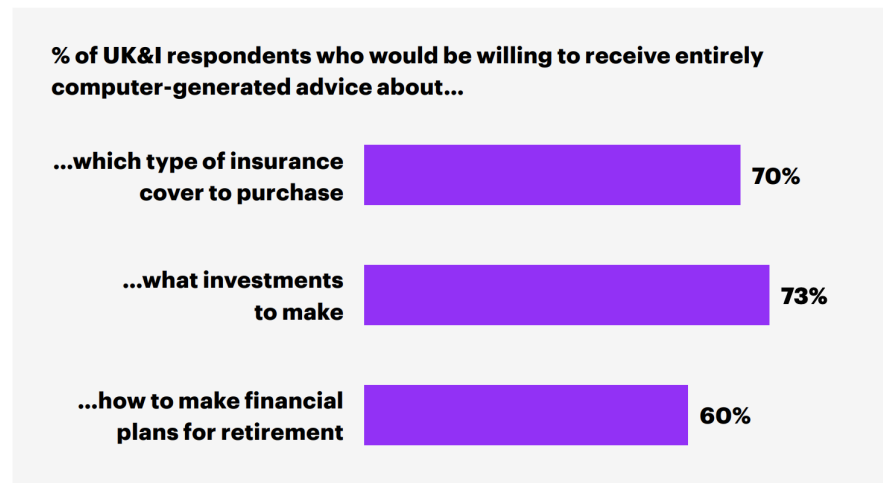


Figure 2: Data from Accenture's FS Customer Survey 2017 (*Accenture*, 2019)

### Block-Chain

Modern technologies pose a threat to insurance firms, as very sensible data is being stolen frequently. *Block-Chain* is the new player in digital data storage on the field and is superior in nearly every aspect to traditional data storage. (such as Databases like SQL, or even Cloud-based Data storage, but even more in the aspect of how interactions are made with the data and how it is accessed from a system. E.g. An HR employee making a request for an employee file functions very differently *under the hood* for traditional methods and *Block-Chain*) Block-Chains are distributed *Data-Snippets* (Ledgers for financial data), and all the snippets together (in a chain) give the constituent parts semantics and context, so that only in such way the data can be interpreted correctly/adequately. Thus, hacking a Block-Chain Database requires an attack on many many computers instead of e.g. a single server-farm, therefore the attack is a lot more complex. Hence, the aspect of security / privacy is interesting for the insurance firm / their clients and worth a consideration of implementation as part of a *digitisation process*.

Cyber insurance growth is constrained by lack of reinsurance options due to challenges in risk measuring, modeling and pricing.

Ask yourself: How can scenario-modeling capabilities be enhanced

with new data and analytical tools?

Some leading players are looking to leverage blockchain technology to mitigate risks and manage cyber liability exposure.

Ask yourself: Which emerging technologies have the greatest potential for cybersecurity applications? (*EY*, 2019)

## Claim Settlement

Two of the most important factors defining the efficiency of an insurance business is how fast it manages to settle claims, and how successfully it does it. Introduction of AI dramatically boosts both of these factors.

A good example of a difference in speed is Lemonade's AI Jim that made the industry news in January 2017 after settling a claim in less than three seconds. This is many orders of magnitude faster than the best human specialist can ever hope to achieve, as it rarely takes the less than a few weeks. (*TechGenix*, 2018)

## Fraud Detection

It is physically impossible for human insurers to gather and process all the information about policyholders that can be an indication of fraud. Companies that rely on AI solutions are capable of processing virtually unlimited amounts of such information, which means that claims are settled not just faster than it is done traditionally, but also with a much lower percentage of fraud. Additional use of machine learning for fraud detection also means that AI learns to improve their results over time, getting the ability to notice the telltale signs of fraud more efficiently as they encounter its new and new instances.

Needless to say, this is a major opportunity for saving money — insurance companies report more than \$80 billion in fraudulent activities a year, and any technology that allows for their better and less effort-intensive detection is a godsend. (*TechGenix*, 2018)

Insurers face intense pressure to enhance their anti-fraud and data security capabilities, as consumers and regulators call for increased transparency. (*EY*, 2019)

This can also be tied in with the above mentioned security aspects of *Block-Chain*. Actual attempts to merge AI and Block-Chain by having the data be *controlled/managed* (where it actually is, how its *fragmented* et cetera) have been made and prove high potential for implementation, especially considering data prone to tempering/malicious activity.

## Key Messages

The Key messages, that inform the company constituent entities about the change, are the technologies to be employed. Those are mentioned above. The key messages also create urgency for the change, signalling the need for these specific implementations/changes. The above describes a general perception of such technologies within the *insurance* industry and the usage/effects of employing them. The productivity increase gained from automation is a significant cost-lowering factor, which is often focused upon when realising change. Thus, there are many/enough arguments for urgency/the need for these change implementations, specifically affecting the IT sector/department of the *RockCity* insurance company.

## Implementation actions

Many of these technologies are cutting/bleeding edge and are not employed as a standard among industries. The creation/implementation of these digital systems would thus probably not be performed internally, but would be outsourced. This approach not only frees resources allocated, but also doesn't add additional required resources (specialised IT labour) to the firm. The immediately above mentioned, is an important consideration when remembering that these systems are mostly customer facing and/or interacted with by non-IT-employees (internally). Thus, there is no necessity for much specialised IT labour.

It would make a lot of sense to do training with non-IT-skilled labour, if there are any left after the "re-structuring/*firing*" process. This training could again be outsourced. My approach to training IT is to utilise *initial training* and *continuous development*. A trainer/coach/IT-specialist could come in and explain the systems to the employees that directly interact with it. The training probably requires multiple sessions to reinforce understanding. Then, employees should theoretically be able to help themselves out individually, without requiring continuous training. The continuous development takes form in collaboration between employees with a differing level of skill/understanding of these IT systems. (*Also die leute fragen/beantworten sich gegenseitig fragen, equivalent zu "der drucker geht nicht, weisst du wie?" - Das wird gewährleistet dadurch, dass man sicherlich in dem mitarbeiter-pool [welcher nach der restrukturierung/feuern neue+alte mitarbeiter enthält] einige individuen hat, welche ein drastisch höheres Verstandniss/skill von/mit IT systemen haben [Welche for dem Change nichth vorhanden waren, genauso wenig die option dieses "gegenseitiges development"].*) (Employee's should be re-positioned/re-structured to complement each other in terms of skills/understanding to minimise [initial] training required for *smooth operation*.)

## References

How AI and data technology are transforming the insurance industry. (2018). TechGenix. Retrieved 4 April 2019, from here

Artificial Intelligence in the Insurance Industry | Deloitte Deutschland. (2019). Deloitte Deutschland. Retrieved 4 April 2019, from here

(2019). Accenture.com. Retrieved 4 April 2019, from here

(2019). Ey.com. Retrieved 4 April 2019, from here