June 2019

The MGA Obstacle Course Cyber, Crypto, BREXIT, AI and Market Reform – What next?

By David Coupe (EC3 Legal) and Kevin Sookhee (Intrepid Tech Ventures)

The MGA Market faces many obstacles but is growing quickly. The MGAA now has some 140 MGA members with over £6bn premium under management – and all within 6 years. However, with reducing capacity, multiple regulatory challenges, new London market practices, BREXIT, and a bewildering choice of improving technologies, these all lead one to ask the question: why be an MGA?

Cyber

Cyber is a challenge for the whole market not just MGAs. Technology is the undoubted way forward – and will only improve. However, this leads to wider issues such as cyber risk. How does one deal with this? Education is still the best defence since most cyber issues arise still from human error. Anti viral software helps – but is always one day behind the hackers and virus developers. There are many cyber insurance products that assist with covering some of the costs and expenses that cover against hacking and viruses. However, these are not and cannot be a complete protection to any MGA.

So where will the market move to make things more secure? What is the "next technology"? A better understanding of the cyber risk market will only help insurers assess new opportunities that can lead to the creation of better insurance products tailored to this market. These new technologies will enhance risk modeling and help insurers expand their offerings into new cyber areas. In the short term, cyber insurance will cater for areas such as business interruption and network and service liability, data and software loss and privacy breaches. Moreover, in the medium to long-term, as technologies help to provide better risk-modeling capabilities, insurers will be able to better assess and quantify losses to intangible assets and areas such as reputation harm, internet protocol theft management could be addressed.

Blockchain and Digital Ledger Technology in an MGA World

These are not now new technologies. Various US insurers have been testing this technology for few years. Jurisdictions such as Gibraltar have Digital Ledger Technology (DLT) Legislation to regulate the use of these technologies, especially in the cryptocurrency world. Imagine though a world where Sterling is a crypto currency, payment is secure, and thoughts of "risk transfer" do not need to apply.

Blockchain is one type of a distributed ledger technology. Distributed ledgers use independent computers (referred to as nodes) to record, share and synchronise transactions in their respective electronic ledgers (instead

of keeping data centralised as in a traditional ledger). Blockchain organises data into blocks, which are chained together in an “append only” mode.

One can anticipate a world when proposal forms, policies, correspondence and everything pass through a secure DLT exchange. However, it is not until the banks have fully integrated DLT payment systems that this utopian world can operate.

Even using DLT, this can give rise to “crypto risk”. Much is being said about this, but there is currently little understanding. What are these risks? There are many of them. We have recently seen the owner of a Canadian crypto exchange die in suspicious circumstances, and he was the only one that held all the codes to some $120m of cryptoassets. One could say that this is bad corporate governance, but fidelity risk and even contingent life risk where an employee dies or loses the “nuclear codes”, or even sells them, is a real risk.
Every IT system has a “back door” – what if hackers break through that door? Cyber risk still exists. And with “quantum” computing potentially on the horizon, will any data be safe? What new safeguards will be required?

Government seizure or control over the servers, is becoming ever more possible as China and Russia try to gain control of “their” Internet.

Further, simple IT failure or physical destruction should not cause an issue due to back up systems being in place – but if they are off line for any period of time, financial meltdown and loss could be significant. If there is non payment, will insurance be available on a credit insurance policy basis say after 180 days? There are many challenges and opportunities about building a blockchain environment.

“Smart contracts” involved in DLT environments are still new and untested. Which law applies and how easy will they be to enforce? It should be added that a smart contract is NOT a contract that the lawyers will understand or recognise. Indeed, it is simply computer coding and not a contract at all. How will the law adapt to cope with this is unclear – and will it be universally understood across all jurisdictions in the same way?

Artificial Intelligence (AI)

AI is “intelligence” demonstrated by machines. Colloquially, it is applied when a machine mimics "cognitive" functions that humans associate with other humans such as "learning" and "problem solving”. It has been with us for many years – for instance, modern chess programmes compute far more permutations that the greatest grandmaster could ever do. They have become almost unbeatable. And yet, their programmers have nothing like the skill of such grandmasters.

However, the truth is that machines don’t learn. What a typical learning machine/ algorithm does, is find a mathematical formula which, when applied to a collection of inputs (the training data), produces the

desired outputs. This algorithm has the capacity to analyse the underlying data (inputs) and find the most important features or attributes of the data which can then help in building a predictive model. One of the most important aspects to understand here is that this process is not static, it is dynamic.

As an example, if we wanted to analyse the pricing structure of a motor insurance company who has 1m customers with customers above 50 being the biggest segment of their market, using traditional analysis, we would create a static model (GLMs) and then use this model to estimate premiums for new customers. Using AI techniques, this process differs. As our pool of customers increases or decreases (1.1m in one year or 0.9m in one year), the demographics of our customer base changes(maybe customers below 30 are now our most important segment) and as such the underlying features and corresponding weightage of each variable impacting our model continuously changes and this process is dynamic.

AI is coming into all areas of day to day life. In some areas it will be slow – in other areas it will be faster. MGAs need to understand how AI may reduce or increase risk, how this impacts on pricing and claims and on regulation, and indeed, whether this creates a wider operational risk which impacts solvency capital.
Does AI create a different type of PI risk? What if AI "gets it wrong"? "To err is human…." – so presumably a computer cannot "err". This is fundamentally wrong. A computer is limited by how it is coded, what it is permitted to develop "intelligence", what parameters are placed on its authorities, and the data that is inputted. If this is imperfect, then the computer may err. If one simply says 2+2, we would naturally say 4.

However, if one doesn't ask "two of what", then we can naturally err to the wrong conclusion. Put simply - 2 apples and 2 pears don't make 4 apples or 4 pears. It is a matter of programming that tells one to ask the additional question. The problem with AI can be that if the computer is told the first time that they are apples, it may assume that they are apples every time… when they may not be! This is terribly simplistic but does show the limitations. Sophistication will grow, but one can anticipate gaps in knowledge. As an analogy, if we teach an algorithm to learn about dance music, you cannot ask the algorithm to play reggae music!

How does AI develop empathy? Computers operate in code. They don't have empathy. They exercise mathematical binary judgment – it is black or white. What if it is not black or white? What happens? What if the claim is patently valid on the parameters set of it – how does it interrogate the know facts to ensure that there is no fraud being perpetrated?

- What the impact of AI will be?
- Where it is most likely to hit i.e. which markets?
- When?
- What insurers are doing?

- What they will be required to do?
- How much it will cost them?
- What new IT they will need if anything?
- What impact on PI?
- Social Effect
- What impact on employee levels?

Insurance issues are tricky as the potential stakeholders in any AI application range from the algorithm designer, coder and integrator and the owner of the data sets, to the manufacturer of the product using them. AI can reduce risk but won't remove all inherent risks to the product. Depending on the complexity of the tasks involved and the ability of the AI algorithm to learn these patterns and the demographics associated with the industry, AI can be extremely useful. Aon have announced how they are partnering to look at vast quantities of historic data to see how AI can be best used. This is a huge step forward, but the value of such data here is really dependent on how well the AI algorithm is programmed and used.

The algorithm having the ability continuously to learn about the different tasks has the possibility to eliminate menial tasks and perform standard tasks better than a human. The more experience that we have, then the better the application of the AI algorithm will be. For example, if a cardiovascular doctor diagnoses that a patient will have a heart attack depending on a specified category – e.g. patients over 50 - but the same doctor decides to use the algorithm to test patients under 40, are the results valid? In such a case, if the same doctor wrongly diagnoses the patients under 40, who is responsible and liable? One could argue that the algorithm has been tested before with all over 50 patients and should therefore give an approximate result. This example raises the following questions: Do AI tools need to be certified to perform the same medical tasks as a human? And what insurance is available in case the advice is given by an algorithm and causes physical damage or financial harm?

Issues are more complex when we consider professional services firms such as solicitors, lawyers accountants, insurance professionals etc. using AI to provide services to their clients. There will be obvious gaps in coverage insurance wise as new situations arose where the apportionment of liability belongs. Moreover, clients are often not aware of how AI is being used in providing them services and consequently, some of the risks are hidden. Depending on the professional firms industry and the complexity of the tasks involved, AI has the potential to minimize professional indemnity risk on a long term basis. On a shorter term to medium term, it is bound to introduce new risks – however these risks can be better mitigated on a longer term strategy as new situations arose which will give the algorithms the chance to learn about these situations and as such improve their accuracy rates.