Russell Group Interviews EmergIn Risk CEO Jamie Bouloux

The MADD World of Cyber Connectivity

EmergIn Risk CEO Jamie Bouloux was part of the team that founded *EmergIn Risk* as an MGA in April 2016 after he joined the start-up's parent company *Ryan Specialty Group* in October 2015. Before that Bouloux started in insurance at *AIG* where he held various positions across the company primarily in the Financial Lines class, after joining as an FI Underwriter in the company graduate scheme. He worked for *AIG* in New York on joining the business in 2009 just as the world was coming out of the end of the financial crisis. Bouloux was tasked with helping the International head of FI with formulating the corrective strategy for *AIG*'s portfolio post crisis and placing its reinsurance treaty.

Russell Group interviewed Bouloux ahead of its Connected Risk roundtable being held in the Old Library at *Lloyd's* on the 18th July. In a foretaste of the upcoming debate we asked Jamie about his introduction to the world of emerging cyber exposures and the impact of connected risk across the Specialty classes.

***Russell Group* (RG)**: **You joined AIG at an interesting time. Describe your introduction to the world of insurance**.

Jamie Bouloux (JB): Obviously the D&O class had been hit significantly but it was the FI PI, FI Crime, and even FI D&O portfolios that had been more adversely impacted on a global basis. This was certainly due to the financial crisis but compounded by the Bernie Maddof Ponzi scheme. Then I was challenged with finding out why cyber hadn't worked in the international markets but had in the U.S. That was my introduction to the new world of cyber insurance.

We discovered that the policy wording we had in the international market was relatively archaic. The increase in legislation in the US was ultimately the main factor in the growth of cyber covers before it went mainstream. The prime driver in this emerging risk was tied to notification. Businesses were compelled to notify data subjects. That led to digital consumers effectively ultimately having new (digital) rights.

At the time, however, the biggest cause of financial loss in the U.S. due to cyber was the cyber event management, in the wake of the notification, to inform individuals that their data had been compromised.

Business had to write letters and post them to those individuals that had been affected. The average cost was about $4 per letter including postage. The costs stacked up quickly. Credit monitoring insurance and identity theft insurance were an important part of the proposition. Another key driver was the litigious nature

of the U.S. The plaintiff's bar was becoming bored of chasing traditional SEC actions, was hunting new prey, and cyber and data privilege became a new part of the legal diet.

To date a lot of cases have been thrown out; but whenever there is a new data breach you, can be guaranteed that there is a class action pending.

Then Business Interruption became the big issue in cyber. The proposition to risk managers led more to rationalising physical BI and non-physical BI, identifying what the exposures were to the organisation - not just for the property burning to the ground but say the network being on fire and what that meant for organisations' ability to quantify their risks.

RG: What does the cyber landscape look like today?

JB: Looking closer to home in Europe, data subjects today in theory have to prove data loss led to financial loss to be able to take action against the data controller/processor but ultimately the new GDPR allows them to sue for punitive damages.

Ultimately how the breach occurs, the type of data that is breached and how a business facilitates the security of that data, will be very important. Don't forget the secondary or 2% or $10m fine, whichever is the highest, for the ancillary elements of securing a business network and doing everything possible to secure data and prevent it being accessible.

It is important to devise a strategy for preventing wide scale denial of service attack through to managing how effective the organisation is in managing failures. It's not just about the security but how the organisation is managed, its culture, as well as the scope of technology that is used.

RG: What is the *EmergIn Risk* mission?

JB: The modern-day organisation needs to consider the exposures around technology and having networks that run across their company. That is the reason why *EmergIn Risk* was formed; that is our mission. Our philosophy is that we can't apply one-size fits all propositions to *FTSE 1000* or *Fortune 500* businesses.

If you are a manufacturing organisation, your cyber exposure stems from running large management operations and processes that connect with distribution and massive logistics facilities.

Then look at the airlines. A major exposure for them is the fact that 95% of ticketing is governed by two organisations – *Sabre* or *Amadeus* – so it is easy to identify the single point of failure exposures that brings. What *EmergIn Risk* does is put together an application form for an airline that asks, "What is your average loss on a daily basis if you can't fly your planes internationally or domestically? What does flight crew cost look like? What do fuelling costs look like?" We then help them identify their exposure.

Then we move onto Financial Institutions. We ask a bank "what is your true loss in the event of a network interruption?" A bank earns money in two basic ways; one is investment income and the other is non-investment income. If the system is down for a week, there is going to be an impact, though not so much on the investment side because a lot of the bank's positions will be long positions. Loss of fees is a potential loss maker if the bank can't execute a trade. We can pull all that information out of a public filing to learn what a loss exposure is for a bank if they're down for a day or for 6 days as happened with *NatWest*. Our aim is to create tangible solutions for risks that seem to be intangible.

RG: How do you help your clients to identify these intangible risks?

JB: We identify the industry that the client is working in, assessing the failures that could arise in a more holistic way - what are the potential single points of failure? So, in manufacturing, it's seeing that *SAP* or *Oracle* control huge amounts of the processing within industrial control systems. So you already have two single points of failure there. If somebody were to work out how to hack in to their network or create a software bug or malicious code against one of those vendors, there is potential downtime; so we ask probing questions.

A simple question to ask is "why are you buying cyber insurance? Are you buying it for a catastrophic loss exposure or because you perceive a risk is more of an attrition threat?" A facility might be taken offline, which means that a business might have to increase production in another facility to meet demand; then there are increased costs associated with shipping.

RG: Moving onto connected risks, what are your thoughts on that threat?

JB: Cyber, for example, is having an incredible trajectory. *Lloyd's* survey of the biggest risks it faces also focuses on the political volatility of the landscape we live in. An organisation might consider itself squeaky clean but if a group of activists or terrorists perceives you are an actor of the state or simply even if you reside in the U.S. or UK, you can move onto a hacker's target list for reasons that seem unfathomable to you.

There is a growing understanding of the fact that individuals and business are no longer in control of their digital footprint. The worry is that somebody will see your digital footprint and extract something from it not simply because they are out to make a buck but because of a broader scheme. It could be that the business is a key player in a local economy or industry that conflicts with hacktivists interests or ideology. That is a growing concern for organisations and stems from the new risk of growing interconnectivity.

Organisations face political or geographical constraints. If you are in London, you sit on the national grid for electricity and use *BT* for your service providing, you might outsource to *Amazon Web Services* for your data hosting. You are now affected multi-nationally by: a) circumstance of where you are, and b)

circumstance of where the best vendors in the world are. So the risk quickly starts to add up and overlap.

RG: Is the problem of an economic risk such as global debt or mounting debt in the newly prosperous Far East intertwined with cyber? Is that something that worries you?

JB: Yes, but for different reasons. There are different reasons why the rise of China might be a problem for our clients, one example being the theft of IP. The question is ultimately how do you begin to quantify the impact of that theft. We are starting to see some really good ideas as to how you build a model that quantifies loss; one idea is a kind of arbitrage between expected revenue and what a business might have actually earned - but failed to - due to piracy.

That works nicely for clothing brands, but it's harder to achieve if you are an engineering firm and somebody in China steals your bridge model or engineering plans. You don't have much room for manoeuvre in that scenario, and you probably would not have got that job anyway so it's moot whether you suffered a loss. Is there a loss to you, it is hard to say. How do you quantify the economic loss? We're looking at that, however, no doubt.

The other issue is the political environment in China where they are starting to introduce regulation around their data protection laws, which they did 1st June this year. They have introduced their own standards; we say to our clients that this is a big issue, the same way we think GDPR is a big issue for any organisation in and outside of Europe.

Organisations outside of China are at risk now because they have to secure the data of Chinese nationals. Failure to do that could result in a business being kicked off their network completely.

The issue with Chinese political regulation is that it is not transparent to us, and we have concerns about some form of nationalisation of your data. Imagine you are processing Chinese subject data, you fail to secure it efficiently, and as a result the authorities take the punitive step of nationalising your servers and take control of your data. That is the risk we talk about when it comes to China.

It is a big concern because it will affect the world and create a global shock. When you get a global shock, then organisations have to tighten their belts. Unfortunately the IT and the back offices are the first places to be affected because people will always skim from that rather than the producing elements.

Ultimately the world we live in today is about securing your producers, securing what they need – which some people may consider a bit short-sighted – but that is the way it is. People want to sell product so they cut from the back to move forward or out. Once that happens, it creates big holes in the back-office IT security, which creates risk.

The recent example was the *BA* crisis where it was reported that they had let go 200 security and IT consultants, so the cry went up that the company was negligent with regards to its controls. From a D&O perspective, the risk starts to mount very quickly.

RG: So, if investment in IT drops that alerts your risk radar?

JB: Yes, there would have to be a reason for it. That is why when we underwrite we look at the financials. There are key metrics we look at to understand that if the liquidity position were to change for this organisation, what does that actually mean?

When you look at cyber, you look at it two ways: one is the technical element - understanding the data assets in the network, where they are in the network, what they do and that important technical element. The second piece is management and culture, which I sometimes think is more important from an underwriting perspective. Even the best firewalls can't always prevent a data breach. If a CEO or CISO does not understand why we are probing them on their internal controls and culture, then that should be a concern.

Another aspect of our interconnected world is the idea that traditional perils or policies are potentially going to be exposed to cyber in ways they never have been before. Take property. We understand traditional fire and flood, for example, we always ask, "have you got water sprinklers in your building, or did you build your facility on a flood plane?"

We understand those issues and can model the risks, but connected technology in factories, for example, expose manufacturers to emerging risks. Going back to the fire sprinkler, building management systems across an entire city are now exposed to hackers taking control of water sprinkler system and demanding extortion. The other scenario is simply hacking the company and taking control of sprinkler systems by turning them on to cause damage purely because they have a grievance against the business.

The traditional way in which the property policy was written was to cover elements of loss from a systemic exposure, which we understood such as a storm is being challenged by the way we construct buildings and the way we live and work today. In the world of the IoT, we are now more exposed today to the traditional perils than previously.

There are so many questions to be asked around this issue of interconnectivity whether that is political or economic, cyber or terrorism, physical or non- physical, which is being driven by aggregation of data in this world of expanding volumes of data.

RG: How will GDPR affect your clients?

JB: The thing that is so interesting about GDPR comes down to when you talk to a client and explain that the *NSA*– for all its resource - couldn't keep its secrets

secured, therefore why do you think you can keep yours out of the public domain? GDPR standards are vague. GDPR Article 30 *Records of Processing Activities* and Article 32 *Security of Processing* outline high level security protocols that businesses should undertake, which are to adopt the best security standard(s) that would be expected to secure the assets that are being stored.

There should be direct correlation between asset and the security infrastructure required to support it. The language around GDPR is opaque, however. The question of responsibility will ultimately come down to the local data protection agencies (DPA) and their judgement as to whether the business protocols were sufficiently robust in terms of securing the data.

When public agencies are determining whether your own security infrastructure is effective, are you comfortable enough to say that you did everything you could to secure the asset, based on the standard that they proscribe, knowing there is a 4% of global turnover fine on the other side? It is not clear yet, but certain jurisdictions are saying that they will be able to eat what they kill. If your data protection agency is going to be eating what it kills, there is every prospect that they are going to be killing large beasts.

RG: There are 8 "rights" under GDPR, so are we creating a new form of human digital rights? So, if there is a massive attack with millions of people being affected could that be seen as a digital crime against humanity?

JB: It's funny but I had this conversation not long ago with an agency. I think it is not unrealistic to see it that way at all. I think cyber experts are viewing it that way. What we are seeing, however, is a de-sensitising of people's fear of these events because they happen so often. When we see Wannacry being pin pointed on North Korea - one of the biggest weaponised attacks that we have seen - it shows there is a dynamic shift in the capability of the people that want to execute these types of attacks.

The first of these kinds of attacks was Stuxnet, which was a very aggressive position because it was about sending Iran's nuclear enrichment programme backwards, which is a powerful statement. Now, in theory, we have North Korea launching these types of attacks across the globe.

In my conversation with the agency, we discussed how the cyber threat is the fourth vector of war. When a (reportedly) state actor launches Wannacry shutting down the *NHS*, it is directly affecting innocent civilians in a time of cyberwarfare, which in theory could be seen as a breach of the Geneva Convention. It is a great question: at what point do we hit the tipping scale?

Put it another way, when do the scales tip to the point where we say: "You know what? If they are willing to do it, we're willing to do it to them." Then they are going to do it back to us, and we just can't shut this down this cycle; it just becomes a bigger, faster digital version of a nuclear arms race. It's like Mutually Assured Destruction (MAD) or its digital equivalent Mutually Assured Digital Destruction (MADD)!