The Impact of Connected Risks on the Insurance Markets

Tuesday 18th July 2017
The Old Library at Lloyd's

The Impact of Connected Risks on the Insurance Markets

A high-level executive briefing on the perils of connected risk to the global insurance markets was convened at Lloyd's of London on 18th July.

Hosted by Russell Group, the forum heard from experts at the cutting-edge of insurance, reinsurance, business risk analysis, cyber-attack prevention and protection.

Over 100 senior industry figures, including from Lloyd's syndicates, risk management firms, the Bank of England, HM Treasury, Fortune 500 companies and top international business and sector-specific media including Financial Times were drawn to the event at the historic Old Library at Lloyd's.

Meet the Panelists

Suki Basi (SB)

CEO of Russell Group Limited.

Suki Basi is CEO and founder of Russell Group Limited, a leading risk management software and service company which provides a truly integrated risk analysis framework for (re-)insurers and corporate clients operating across multiple industries and geographies.

Dr Adriano Bastiani (AB)

Head of Casualty Facultative for Global Clients North America at Munich Re.

Adriano Bastiani is Head of Casualty Facultative for Global Clients North America at Munich Re.

Luca Berni (LB)

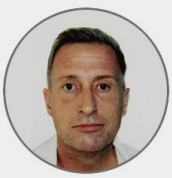
Analyst in the Cyber Threat Intelligence team at Control Risks.

Luca Berni is an Analyst in the Cyber Threat Intelligence team at Control Risks, where his focus is on researching sophisticated cybercriminal threat actors, and on analysing the geopolitical motives of cyber espionage. Luca is a Certified Ethical Hacker and has a BA (Hons) in International Relations, gained in Italy. Luca holds an MA (Distinction) from King's College London, where he read Intelligence and International Security.

Jamie Bouloux (JB)

CEO of EmergIn Risk.

Jamie Bouloux is CEO of EmergIn Risk, an acknowledged and well known cyber expert in today's highly digitized and connected environment. Jamie has worked on developing unique cyber solutions alongside brokers and clients across the globe in his present role, and also whilst he was Head of Cyber at AIG EMEA and lead cyber underwriter at CFC Underwriting.



Richard Brown

Panelist Chair

Richard Brown is a Business journalist, writer and presenter, having worked for leading media organisations in London, New York, the Middle East and Asia.

We live in a world where the Internet of Things creates a new form of connected risk. With the multiplicity of connected devices, which according to Gartner connects 6 billion devices, what sort of risk profile does this pose for our industry?

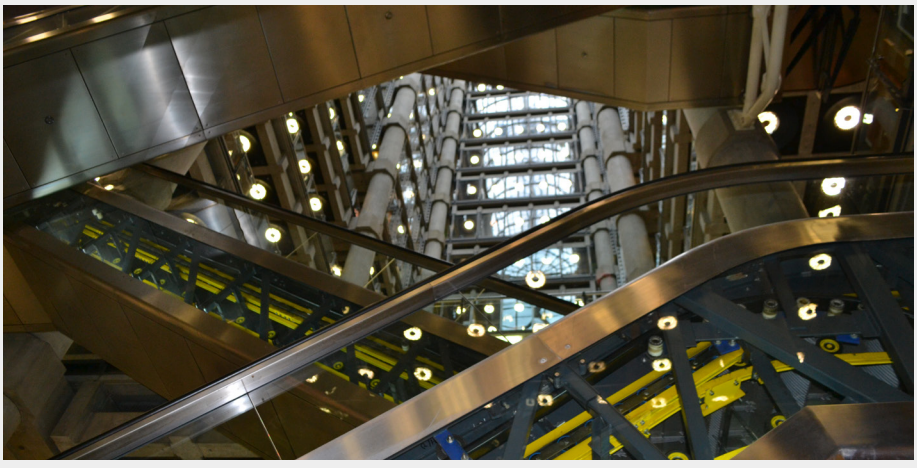
Luca Berni (LB): I would like to begin by looking at the benefits of the Internet of Things (IoT) to society. These are particularly obvious when looking at the potential advancements in terms of automation, remote control and access. However, we have observed misuse of the IoT. For instance, hundreds of thousands of compromised devices combined into the Mirai botnet to brought down a DNS provider in October 2016. The end result was to render services like Twitter and Paypal unavailable to users for a relatively prolonged period of time. This is a real problem for e-commerce businesses whose profitability is dependent on the availability of web services. We are seeing the same Mirai botnet being used for extortion purposes by threat actors against financial services organisations. In general, we are increasingly relying on connected devices in our daily life. Think about cars, planes, and medical devices all of which are connected to the Internet. The issue is whether the benefits outweigh the risk and how can we make sure that these devices are secure by design.

As more devices become more linked what does this mean for the business world in which we live with all the vulnerabilities inherent with connectivity?

Dr Adriano Bastiani (AB): I think the key take away of an analysis of 2016 is very simple: the world is changing rapidly. Looking at the answers to our survey, the cyber threat ranked most important according to respondents. If you looked at research from 10 years ago this cyber risk wasn't there. The second aspect that is not really a surprise is that BI [Business Interruption] is a predominant theme throughout. Keeping the business running is a key concern. With supply chains becoming more difficult to handle because of silos this risk is definitely increasing for enterprises.

On the other hand, traditional risks like human error, quality of product, technological progress are at the bottom of the list so we are turning this risk landscape upside down. We have to ask the question: "are we overestimating some risks here or underestimating others?" The result is the same: we have a dramatic change in the structure of the world economy and this is changing the risk landscape of re/insurers' businesses.

Jamie Bouloux (JB): I see an element of risk concentration



as being one of the big issues. BI is a major challenge so mitigating that threat vector is very important, particularly for SMEs. For example, these businesses are more concerned with general market developments because they are more exposed to recession and they have a limited risk modelling capability vs. large organisations. Many SMEs will be trading on the high streets of a local geography so if events develop adversely [whether economic or natural catastrophes] smaller firms are affected quicker than larger organisations, which are more able to diversify their business and supply chains, having gained valuable experience attacking traditional risks for a lot longer.

PwC conducted an analysis of the 100 biggest companies by market cap. An interesting sector within that list is consumer services. In 2009, during the time of the financial crisis there were only three global consumer services: Walmart, CVS Pharmacies and McDonalds on this list. Fast-forward to a similar list from 2016 there are now eleven. The biggest new entrant is Amazon that surpassed Walmart, which has fallen down the list to 18.

We have further seen entrants like Alibaba and Walt Disney, these companies are challenging the traditional brick and mortar business models bringing consumer experiences and content into new era of digital distribution. We are seeing that online market places and digital content distribution is shifting and so is the landscape for how large organisations are looking at their digital risks. And as such, it is no surprise that the risk barometers for large organisations has shifted from traditional concerns around employee risks to technology risks.

Suki Basi (SB): The complicated and connected nature of risk for modern companies threatens all risks across all the Specialty classes. We have seen this develop in recent history, from the Thai floods, Sandy, Tianjin to WannaCry, events are becoming more complex, but the key difference is that they are more connected, bringing in more product classes into the same event. So, we need to find ways of putting together a framework and representation of risk that describe all the receiving classes of exposures that are driven by the classes that surround them. We need better clarity of data: that is the key point. Not only is the connected nature of risk creating more complicated risk profiles but, as an industry, we need to react to that threat and understand the underlying risk for what it is. The key to this is not just data but the way in which we book data and classify risks as an industry.

What is the risk to enterprise management?

JB: Something that Suki and I have talked about at length is the idea that the biggest threat to organisations is not embracing a culture that embodies change. As we move into the Fourth Industrial Revolution change is happening faster than we have

ever seen before. Processes are changing, therefore risk engineering must change. Looking at factories as an example, in the late 1800s factories were concerned about disease, fire etc. In the 1900s the concern was about the loss of labour force during the great wars. In the late 20th Century and into the 21st it becomes more about industrial control systems and disruption to those, whether that is due to malicious intent or system failure.

I gather that there are even conversations taking place among risk managers about what kind of Pacemaker their CEO has - we have moved into an era in which we can potentially hack Pacemakers! How do you manage that from a risk management perspective?

Globalisation, supply chains, the use of outsourced providers, sharing data with third parties to give access to our clients and new economic shocks are being felt throughout the world faster than before. That means there is increased scrutiny around capitalisation and shareholder shock concerns. The reality is that the client's exposure is less physical and more abstract, non-physical, which is difficult to identify. We need to find ways of looking at what contagion looks like in the cyber sphere. Look at people alone, how do we find the right people to help us manage this risk? That is the biggest issue, the talent deficit.

What about the reinsurance risk?

AB: The insurance business has always been looking for non-correlated risks. In an interconnected world, however it is becoming more difficult. It is becoming more difficult to maintain transparency of the risks, and understand what you have in your portfolio. As a reinsurance company we are gathering multiple exposures from multiple cedants and that will impact on our balance sheet. You may say that this is what we have always been known but the degree of effort that is necessary to keep transparency and understand the correlation of individual risks in your balance sheet is increasing dramatically.

Is this just another Y2K scare? Is connected risk an over-hyped and exaggerated cynical ploy to promote fear mongering? What is the difference between connected risk and Y2K?

SB: It is similar but different. Both exposures are similar in the sense that there is a lack of investment in certain areas but the connected risk is different in the respect that this is a new reality we are faced with. What is needed are business

models that are aligned with the risk models. Enhancements are required to systems and processes to mitigate risk and deal with the opportunities.

JB: We are starting to see how connected we truly are. I think in 2000 we were all counting down and looking at the toaster to see if it was going to kill us or not! The realities of today's day and age is that we have serious interference with nation states, whether that is Russia using the Ukraine as a test site for weapons or cyber weapons or the issue with WannaCry. Then there is the wide scale DOS[Denial of Service] attacks against the banks in the U.S. through to critical infrastructure being disrupted by the IoT. That is the reality of this age. It's no longer science fiction.

What are real life examples? Say, WannaCry?

LB: When I was asked to present here I wanted to show something that happened quite recently. On 21st June

2017 Honda, the Japanese car manufacturer, was hit by the WannaCry 2.0 Ransomware campaign. There is a cyber and technology element to it, which is the technological exposure to known attack vectors and their ability to halt the production of the factory floor for one day with the loss of about 1,000 vehicles. That likely led to a severe financial loss. We have an operational disruption in a physical environment but where does the attack come from? It is likely linked to an Asian country. Why would a nation-state target a private company for direct financial gain?

There are increasingly strict economic sanctions imposed on the country, which leaves it needing foreign cash. How do you get cash if, like that country, you are cut off from the global system? One possibility is that it developed this malicious software to raise funds. They likely did not achieve that goal but then again we need to understand the geo-political environment to understand the motives behind the cyber threat. A further element is that threat actors behing Wanna Cry 2.0 used a sophisticate exploit to infect systemsthat was likely developed originally by a Western country, and then likely leaked by a third country.

So you have an interconnection of a geopolitical environment that affects the behaviour of a country, which in turn brings

operational disruption on a factory floor to a company that operates in a country - Japan - that is a geopolitical rival of the country likely being the WannaCry infections. The main point is that we cannot look at the cyber risk in isolation: we also have to take into consideration the economic and geopolitical environment in which it operates.

That brings us onto geopolitical risks and so the Hanjin episode when that company went bankrupt and how that affected global trade.

SB: Hanjin was a top ten cargo operator operating in a hugely competitive environment shipping in excess of 100 million tonnes of cargo. At the time of its bankruptcy you had vessels stranded in different locations either not able to leave port or arrive at port causing events that involved no property damage but huge liabilities. Whether that is defaulting by firms not paying out and causing a loss to the credit insurance industry or business interruption to retailers not receiving supplies in time or even inventories for manufacturers that were unable to manufacture “just in time.”

Just prior to this briefing, there was also another example in the logistics industry at Maersk, which came on the back of the ransomware attack earlier this year. Its logistics were interrupted when systems were brought down. For a period of time it could not operate, so the logistics industry, which is at the heart of the global economy and hugely competitive, is considerably vulnerable to connected risk.

So global shipping grinds to a halt and people don't get perishable goods, which languish at sea and the contingent losses are horrendous. Hanjin is a tangible example of the connected risk world we find ourselves. Technology lies at the heart of these issues.

AB: Did I mention to you that the world is changing? You can see the market capitalisation of companies in 2006 then witness the difference 10 years later. You see where the money for investments goes these days. On the list 10 years ago you had big oil and gas production companies from top financial institutions while big technology company Microsoft was in the middle. 10 years later we see 5 out of 10 companies that are IT focused or IT related.

Besides the market cap of these companies being 50% higher than 10 years ago there is a huge shift from products to services. Capital is going from production sectors to service sectors with completely different vulnerabilities because they have a high degree of inter-connection. If you look at the top companies, the Apples, the Alphabets and Amazons, these companies are serving the whole world economy or are in some way linked to it. The big take away from the insurance industry perspective is that we will need to adapt to that new reality if we want to stay relevant.

We have to understand what is going on out there, how these companies are changing and what the necessities are. We need to understand how these companies are interconnected and what it means for our risks. By the way, and this might sound provocative, we have to ask the question: "do we have the right skills to do that in insurance?" To sum up, the world is changing and we need to stay on board the fast express to connectivity if we don't want to miss out.

Describe a possible or probable event – a space storm, which could knock out global communications. What are the potential consequences for the global insurance industry?

JB: What we're looking at is the consequences of solar storms that ultimately are the by-product of what happens when there is a major solar flare? The result is a mass of x-rays, charged particles, and magnetic plasma that rains down on the Earth and interacts with our atmosphere. Solar flares are rated like earthquakes so you have a C-class, which is what happens on a daily basis. You also have an M-class, which is where you start to see interference with radio frequencies. Finally you have the X-class, which is the biggest example of an explosion in our solar system that is equivalent to a billion hydrogen bombs exploding at one single time. Solar flares are highly unpredictable.

The issue is that we have a hard time understanding the magnetic field around our sun. At the top of our magnetic field an isopheric current occurs when that element of the atmosphere becomes too charged. GPS satellites' ability to function would be scrambled at this level, so as soon as you get a frequency that disrupts them you no longer get a

handle on the GPS positioning. This is a big concern for aviation underwriters because we are moving further into the era of GPS on all of our airplanes.

Beyond that you start to get issues with radio being interrupted so how do airlines communicate with their central control systems? It's not uncommon, when planes are travelling above the poles, for magnetic fields to disrupt the ability to connect with control centres in the traditional satellite way. If solar flare activity is too bad the authorities will not fly planes.

The biggest solar concern is coronal mass ejections (CME).

These events cause massive geo-magnetic storms at the top of the atmosphere that result in a build up of electrical currents on the ground causing conduction. There needs to be an exit point for that charge, and if that doesn't happen there could be a surge in the power grid that might explode transformers because they wouldn't be able to convert the electrical volts into the grid.

The fear is that, depending on the size of the CME, it could destroy all the transformers in the power grid. What does that mean? There was a smaller example that occurred in 1989 in Quebec that led to a 12-hour outage and then another event that occurred in 1859 which is considered a monster storm: the Carrington event.

Carrington is the astronomer that identified the event cause. The world was lucky that we weren't as interconnected then as we are today. The Carrington event disrupted all the telegraph poles and communications were halted. The technicians that were working on the telegraph poles at the time were blown off the masts and in certain communications centres there were fires where the papers close to the equipment were burnt.

What is the viability of that happening today? In July 2012 our planet missed a monster storm, which missed us by 9 days. The implications could have been severe for the world. A National Academy analysis revealed that if the event had hit us it could have led to 4 years of reconstruction trying to get broadcasting telecommunications, power networks and GPS back online and the value of that cost was estimated at $2.6 trillion. Space weather is a big concern. It is not unrealistic that this event is going to occur. The experts say that, as far as they can tell, space weather goes through 12-year cycles and that between 2012 and 2024 there is a 12% chance of such an event happening.

Audience Question:

How good are entities at tracking exposures at the other end of the scale, within the casualty class for example? Property is obviously good at tracking accumulation exposure for that class but how good is the market looking at Casualty?

SB: It is very patchy and inconsistent. Some people are doing it very well, others not so good. There isn't a senior management drive to get on top of cyber casualty, for example, though on one level you would expect that to be the case. That may be due to other priorities at the time but as we get into the detail of connected risk in casualty, the industry needs to improve because the underlying industries are becoming more complex.

AB: From my perspective looking at our casualty

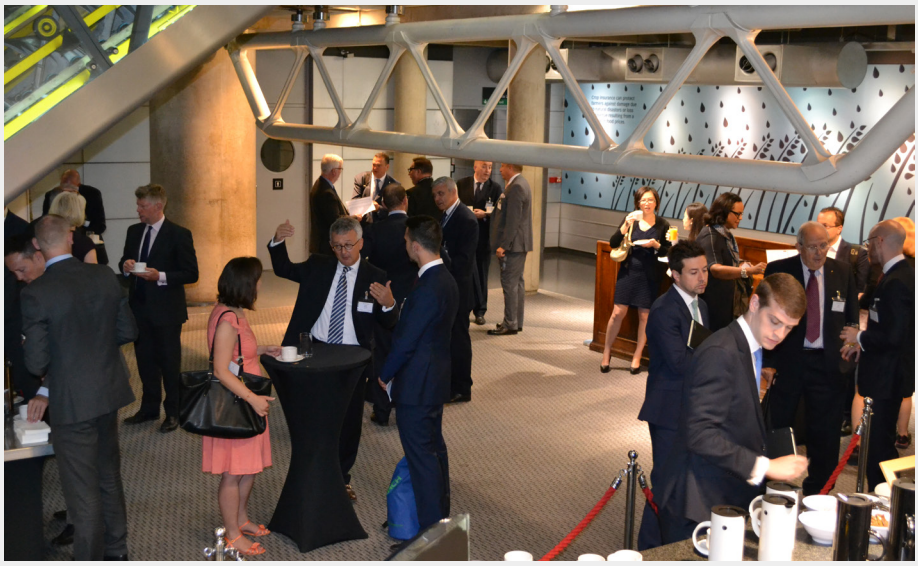
community of insurers I can tell you there is some concern in our industry. What we are doing regularly in our treaty business is to run accumulation controls internally with information that we get from cedants, which is one year behind. I'm proud of our set up but for the rest of the industry we see lots of inconsistency.

You might get information from one client with differing risk information for the same risk (e.g. there is a changing of the name or some other risk information is changing). We receive heterogeneous information from all over the place, but there is a lot more that needs to be done to achieve transparency in aggregating exposures within the reinsurance portfolio. We haven't seen the black swan casualty event yet but with the pressures associated with 21st Century economic development I think we should put more emphasis on this topic.

Audience Question:

Does the industry need a new risk vocabulary?

SB: There is a blurring of coverages between the product classes, like war, cyber, political risk for example, which is being exposed by events that are becoming more complex. Mostly we have been operating in an all risks environment where the events have been traditional



and structured. What that does in an industry where firms have not been coding their vocabulary properly, is that you get this silent cyber threat, for example, moving around the industry and that could be the beginning of a spiral.

JB: The issue goes beyond technology. Not that long ago, we experienced the macro effects of the world financial crisis causing widespread bankruptcy and pushing states to the verge of insolvency. This time created the catalyst for many political movements including the Arab Spring as this time of economic mismanagement was the final abuse against a people who had faced decades of repression. Further, in the 21st Century we have seen fresh water crisis triggering drought in Syria forcing farmers to the urban centers in search of work, causing increased civil unrest in the urban population. This has been cited as one of the causes for Syria's civil war.

We will now dwell on the solution to connected risks and how these might help your business.

SB: As an industry we need to respond with products that are more relevant to our clients in the underlying industries that we serve. The corporate world is becoming more connected so we need to begin by understanding the end client and modern business models better, because enterprises are much more linked than ever before spanning sectors, geographies and clients. The journey to a solution starts with understanding the connections to companies in their supply chain while understanding the geographic locations and political risks inherent there. Only then will we begin to understand the complexity of the risk, the vulnerability and what we as an industry insure or don't insure. It cannot be just on name alone. So need to know and name those risks.

AB: The first step is to ensure that we have a consistent nomenclature, one name for one exposure and one exposure for one name. You have to classify your risks in a unique, more granular way. That is not easy for a reinsurance company because you receive lots of information from cedants, which is very heterogeneous information, everybody using different nomenclatures, formats and systems. To sift this heterogeneous information, you need to start from a point where you have a list of risks that you use internally to match the names of risks that you are getting from the outside.

One example is the Russell Universe, which brings together a fixed list internally and very heterogeneous information from outside. Undertake some matching and you will end up with a list where you can decide if a certain risk does this or belongs to a certain group of exposures. At the very least you will have a solid base to start from to obtain a certain percentage exposure figure from that list. If you know what you have in your portfolio, with more transparency, what accumulations you have then you can much better steer your capacity. This means you can much better diversify your portfolio if you know already what is inside it.

RB: How can you rate or benchmark your connected risk, your vulnerabilities to mitigate exposures?

LB: I look at cyber benchmarking and an element that is often overlooked is how to look at and understand companies' risk profiles. How prepared is a company to mitigate a potentially hostile cyber incident? That means looking inside the company at systems, culture, how good the people are and how prepared they are to mitigate their risks. Also we need to understand what is the threat profile of the company? Understand who may want to attack them and why? How good are they and then look at how appropriate their defences are to mitigate that possible threat?

AB: When we look at benchmarking we look at a tangible corporate profile and throw a series of hypothetical situations at it. Lessons have been learnt and I think that the insurance market is certainly trying to get its head around the challenge of connected risk.

Connect with Russell

Russell Group is a leading risk management software and service company that provides a truly integrated risk management platform for corporate risk managers and (re)insurance clients operating in an increasingly connected world.

Connected risk refers to the growth in companies which are increasingly integrating across industrial sectors and geographies, and creating greater levels of risk. This exposes corporates and (re)insurers to a broader range of inter-related perils, which requires a risk management approach built upon deep business intelligence and analytics.

Russell through its trusted ALPS solution enables clients whether they are risk managers or underwriters to quantify exposure, manage risk and deliver superior return on equity.

If you would like to learn more about Russell Group Limited and its risk management solutions, please contact rborg@russell.co.uk or visit www.russell.co.uk/contactus