Exploring new risks

Last Thanksgiving US retail store Target suffered an incalculable blow to its reputation and business after losing 11 gigabytes of data and the details on 70m customers. In association with The Russell Group, Reactions managing editor Peter Birks discussed the importance of non-modelled non-natural catastrophe risks in the current market with leading market participants.

Peter Birks: A report sponsored by McAfee puts the economic effect of cyber crime on a par with counterfeiting, piracy, narcotics and car crashes. McAfee also notes that most cyber crimes go unreported. Has anyone got any particular view on the state of play at the moment of cyber risk and how it's working in the industry?

David Singh, Amlin: To assist the Lloyd's market with the management of Cyber, the risk code CY (Coverage in respect of the financial consequences, whether first or third party, of breach of security and or privacy of data) was introduced by Lloyd's in 2013 to identify and monitor this important and growing class of business. The reliance on technology, in-house or cloud-based, and the reporting and awareness of sophisticated cyber-attacks is driving the need for tailored insurance and crisis management products and services.

Matt Harrison, Hiscox: It is a strange one, though. To my knowledge, it has been sold in the Liability Market but it's not really third party liability at all, so it must sit differently within that market. And, yes, there is a cyber risk code, but it takes time for new risk codes to be fully adopted, so I doubt we really know what the Lloyd's market premium is, let alone the full market.

Sian Fleming, Talbot: If there is any sort of cyber-attack that resulted in some sort of explosion and therefore fire, you might think you couldn't have a loss because you've excluded cyber. But, interestingly, you're potentially including it back in again with the perils that you write.

Suki Basi, Russell Group: On the cyber products, we did a roundtable at the beginning of the year, the feedback was that actually a lot of coverage was blended. Over the course of this year however there has been a growth of standalone cyber cover, even for big companies. Now, with those companies it can't be treated as third party. It's actually a liability product then, isn't it?

Matt Harrison, Hiscox: I think it clearly is a Liability coverage issue, it's just not necessarily a third party one. Again, I think this feeds back, on the exposure management side, to Liability RDSs. Individual companies will have their own ideas on Liability RDSs, but unlike with Natural Catastrophes, there isn't a market language to describe them, so communicate them. For example, if a Cat 4 hurricane make landfall in Florida we all know what that means, but Liability doesn't work in the same way.

Kieran Heraty, Faraday: But we are seeing cyber as well, even on the property side of it. It is starting to move into policies, especially with the market conditions the way they are. It seems to be that it's almost been bolted on as an add-on, because people are hearing more about it and want to cover it, and it seems to be that big engineering plants where they might be concerned that somebody could hack their systems and stop production will get a Business Interruption plan. It seems to me that that's become more prevalent or that people are looking for that cover.

PARTICIPANTS:

- Stephen Gentili, head of exposure management, Cathedral
- David Singh, group underwriting exposure manager, Amlin
- Kieran Heraty, head of loss modelling and exposure management, Faraday
- Graham Clark, head of exposure management, Liberty Specialty Markets
- Emma Watkins, head of exposure management, WR Berkley Syndicate
- Matt Harrison, syndicate exposure manager, Hiscox
- Sian Fleming, head of exposure management, Talbot
- Simon Webber, head of exposure and catastrophe management, QBE European Operations
- Suki Basi, managing director, The Russell Group
- Peter Birks, managing editor, Reactions (moderator)

Steve Gentili, Cathedral: Well, it's classic coverage creep, and this may continue as the market softens without the required disciplined approach. If it does indeed continue, then I think it will be hidden in PD risk codes.

Simon Webber, UK QBE: Yes, and it crosses the line, as well, between primary and reinsurance business.

Steve Gentili, Cathedral: A potential game changer could result from reinsurers adding a cyber exclusion. That could cause a massive change or shift in focus.

Peter Birks: But it's a softer insurance market, at the moment, so currently there isn't a threat of it being stopped on the reinsurance outwards. So, in a sense, in this particular area of cyber, were you saying it's tending to evolve as add-ons, and possibly add-ons for which there are not being extra charges imposed. How are brokers approaching you about that?

Kieran Heraty, Faraday: I think it tends to be predominantly add-ons as opposed to standalone, particularly for property risks. The

question is whether you want to cover it, whether the BI (business interruption) would be covered with physical damage or without. Then you have to decide the extent of the cover, for example whether you're going to cover all of the software and the data. Yes, it's complicated, and the potential losses are quite sizeable.

Sian Fleming, Talbot: That's why if you had, say, an explosion from an attack that then causes a fire; you could have damage and therefore losses through that. It's not just loss of data, or stopping work that will generate losses.

Peter Birks: Actually, mentioning the RDS there, two questions spring to mind, one being what is the current state of play, and, following on from that, what would people actually like to see as components of that, of realistic disaster scenarios?

Sian Fleming, Talbot: I think it's quite hard to put a realistic disaster scenario around it. I don't think there's enough loss history to create something. I mean, you can go, kind of, Hollywood, and everything goes, you know, planes flying into buildings, everything. Or there are a lot smaller, more realistic events.

Simon Webber, QBE: As you said, Dave (David Singh, Amlin), Lloyd's is taking it seriously, so we can all provide our numbers on a worst case scenario. But by definition on the worst-case scenario, they can't add it up. It's a bit like doing the terrorism accumulations. Your top ten could be my bottom 20. They're non-additive, so if Lloyd's want to get a grip on the market position then it has to be a predefined scenario of sorts. But that might mean, actually, nothing to me. I could have high liability, but based on a predefined scenario it could be minimal.

Emma Watkins, WR Berkley: That's why we have alternative RDSs, so we have internal RDSs and Lloyd's RDSs. There can be a big difference between what's important to Lloyd's, from a market perspective, and what's important to us, individually.

Matt Harrison, Hiscox: And also, do we, individually, believe the Lloyd's RDSs? I suppose that we all "believe" them, but what I mean by that, is are they a disaster for your individual company or just Lloyd's? For example you may have a lot of exposure in New Orleans, but very little elsewhere, therefore the Hurricane RDS events "miss" your exposure, so therefore they're not exactly a disaster for you. Therefore you also need to be thinking about what is a disaster for you and at the same time what you think is realistic.

Peter Birks: Are your internal RDSs more built up from your own exposure side rather than extrapolated from a likely industry loss?

Emma Watkins, WR Berkley: Yes, although they're often adaptations of the Lloyd's RDSs. So for example Lloyd's put a two tonne bomb, for terrorism, at a certain point in New York, but we might know that that's not our RDS, perhaps because we just haven't got much exposure right there. We'll report our numbers to that, but we might also move the scenario to where our exposure is the greatest, and that could be our internal RDS. It's similar with cyber risk. I can imagine that the market might figure out what the biggest policy placed might be, whether it's IBM's policy or someone else's policy, and from a Lloyd's point of view they're going to want to know what everybody's got on that. But, internally, we all have to keep an eye on what our own biggest lines are.

Simon Webber, QBE: Even if they did prescribe cyber, one thing we spoke to Lloyd's about when they first mooted the data call was, is it one event, or is it several events? Because if you have or haven't got your own reinsurance coverage, your net position could be very, very different.

Steve Gentili, Cathedral: Well, I think it's not just cyber. It's the same issue with many types of liability coverage. For example, going back a few years when laddering suddenly appeared and impacted D&O severely, no one had previously allowed for that. With a lot of liability business you're really playing against the American courts, and that's a difficult one to call. Now, cyber is going to be tested in the American courts somewhere along the line, the outcome of which could fundamentally change your view of exposure overnight. So I think your question about the Lloyd's RDSs is one that goes to the heart of the Lloyd's capital models. They've looked at the natural catastrophes in a very granular way and, in my opinion, neglected casualty and the impacts this could have on an entities SCR and profitability.

Simon Webber, QBE: Well, even if you did have a pure scenario, how do you assign a return period to that? And depending whether you're a single year or a multi years, you then start to really look at reserving risk. When is it moving away from scenario, deterministic risk to a reserve risk?

David Singh, Amlin: With Lloyd's operating their RDSs from the market perspective, internal RDSs are extremely valuable as they can be tailored to address a company's specific or whole portfolio based on materiality and proportionality of the risks they write. In the absence of external models for Cyber and similar specialty classes, the use of scenarios can help us to understand exposures and accumulations, with the aim of ensuring a company is appropriately capitalised.

Peter Birks: Moving away from cyber, specifically, what, in the various specialty classes, and non-modelled risk, is the current state of play?

Steve Gentili, Cathedral: I think cyber and CBI (Contingent Business Interruption) are very much linked and part of the same issue. More extensive layers of supply chain exposure data and even a series of losses are unlikely to make this any easier to quantify, and this might only deal with the nat cat element. I think you can only do so much with CBI, unless you model everything on a global scale, That's probably impossible, given the series of events that would give rise to CBI being largely uncorrelated temporally or spatially, given the many layers, interconnections and non nat cat elements involved. In the sense of building a curve, it is very difficult indeed.

Simon Webber, QBE: It could be another coverage, like a casualty loss from an earthquake; that falls under the scope of the NMR (non-modelled risk); it's actually a non-modelled line of business.

Suki Basi, Russell Group: But if we can move away from something like that and look at trade credit and political risks. In Trade credit, premium income's grown quicker than the underlying exposure. Governments over the last four or five years, have actually acted to help that market. But obviously, as time passes, governments are going to want to drop out and actually give it back to the private market. But this is at a time where political risk is actually growing in some countries. But there isn't actually anything in the RDS about trade credit.

Emma Watkins, WR Berkley: There's the political risk RDSs, which include Trade Credit.

Suki Basi, Russell Group: So there is guidance prescribed to actually look at your aggregate in all of those areas?

Emma Watkins, WR Berkley: Yes, and we apply the PMLs that the RDS requires us to apply.

Suki Basi, The Russell Group: And does that run well?

David Singh, Amlin: One of the reasons it runs well is that the LMA plays a prominent role in the design of the scenarios. The LMA Political risks panel – the experts – meets to review, challenge and implement changes to the prescribed scenarios.

Emma Watkins, WR Berkley: It's also coverage that is very easily identifiable. It's written under certain risk codes, and it's pretty difficult to imagine that someone could sneak it into a Property policy, for example. So it's very easy to actually measure how much exposure you've got and where your exposure is. I think it's an easier one to get your head around than is cyber.

Suki Basi, Russell Group: The driver for this was that the cat models have established a principle for the peril side. When it comes to the man-made side, there isn't actually an equivalent. So the purpose of today was trying to understand what people's approaches are, how that's taking account of the Solvency II aspect, and also, whether Lloyd's is actually closing the loop, and developing ongoing RDSs for these classes.

Simon Webber, QBE: The word model is misleading.

Suki Basi, Russell Group: Yes, it is misleading. I think the fact that even the study that I thought was actually embracing outside of cat models excluded casualty lines is interesting. In all these classes I think it's the casualty lines that are possibly the biggest issue, in the sense that they're vast, varied, they have similar properties, the approach are really different, quite different, in terms of how people arrive at what they consider to be their worst position or what internal scenario they're actually using to model their exposure from it.

Simon Webber, QBE: I know Lloyd's were doing a project of sorts with some software house. I don't know what they've learned from that, what the play out in the market is. I think, as we've all said with RDS, if you looked at it our way, Lloyd's have often, it's like we said, we'll start what we think may be a potential risk, and will ask for data, and depending on how they see as a market, we will then expect a somewhat more detailed RDS. Australia had gone from being a top five, extra additional style aggregate to, now they are looking for EP style data.

Steve Gentili, Cathedral Capital: But that's more regulator driven than Lloyd's per se, isn't it?

Simon Webber, QBE: I think it was just a natural thing; if it was always the top one of the other five...

Graham Clark, Liberty: But isn't that how we created this book to business in the first place? We don't decide to go straight to 100 million premium on cyber risk. We dip our toe in the water, see how it grows, see what comes through, look at your line size against your premium income, and you slowly build it up as you get more data, and you take a nice approach to growing up a business. That goes back to talking about the RDSs, how, as the market steps in you'll have a few players who step in; then the rest follow. It slowly grows, and then Lloyd's will start to look at it, start doing datametric exercises and it just evolves through, so that you can understand it.

Suki Basi, Russell Group: So that's saying, some of these lines are still an evolutionary approach at the moment?

Emma Watkins, WR Berkley: Yes, we have to keep collecting data. I think you said, right at the beginning, when we were talking about cyber, that McAfee had done a study saying that they think the cost of cyber crime is 'X', but that eight out of 10 crimes aren't reported. That's just it: we literally don't know the size of the cyber problem. With windstorm we've collected a lot of data over the last 50 years, and much more over the last 20 years, about what size losses can happen. And so even if you know nothing else, you can figure out what your likely market share is and apply it to a potential market event. But we just don't know what a market event is for a lot of these perils, not just cyber.

Steve Gentili, Cathedral: And a few events, possibly.

Siam Fleming, Talbot: And windstorm is a natural thing. It has natural boundaries.

Emma Watkins, WR Berkley: Hardly like terrorism, where you think it's going to happen, they don't do it. You can't predict human behaviour.

Matt Harrison, Hiscox: But what you've said is quite interesting, the fact that would we want to construct something like at cyber, because I think, taking your point about terrorism…

Emma Watkins, WR Berkley: It's going to be spurious, yes.

Steve Gentili, Cathedral: I don't think you can probabilistically model terrorism. As Sian said, natural perils have physical boundaries which can be parameterised; terrorism has too many to make a robust assessment.

Emma Watkins, WR Berkley: Yes, I agree.

Matt Harrison, Hiscox: I totally agree that I'm not sure you can probabilistically model terrorism, but at the same time we've still got to know what exposure you have to it, know what you expect the losses can look like and in the world of Solvency II you have to characterise this within your internal capital model. So you need something that parameterises it. You've got to have something that's your interpretation, so the same should be true of all these other "difficult" risk, in which I'd put cyber. If you believe that you only get this through the one product line, then it can be done through the large loss distribution for that class of business, if not you need to do something more sophisticated. The whole thing will then be potentially similar to what you do with Terrorism – come up with some scenarios that describe what you think the risk is, make sure you stress them, then you can develop things from there...

Steve Gentili, Cathedral: This is the issue about having to do something purely for your SCR because I think there are certain elements of the book that you can't assign probabilities to and have any great comfort in them. To me it's absurd that a vendor creates a model with implied probabilities for terrorism and calls it game theory, I don't buy into it in the slightest, because, as you say, the day after an event the probability for that attack mode diminishes and in some cases ceases to exist. Meanwhile other new threats potentially become apparent, but others remain and build up again over time, for as long as there's not been an event. I don't think we should be het up too much and try to build EP curves for these classes. Yes, we are in the world of the capital model, but I just don't think it's sensible to assign probabilities and build a curve if this is the only form of exposure management used for these classes…what about aggregates?

Emma Watkins, WR Berkley: But you do have to, don't you? For the purposes of parameterising your internal model, and producing

your SCR, you have to assign some sort of probability, somehow, to some loss amount. I'm just not sure you should get those from a probabilistic model. I think the question is where do we get those from at the moment? Mostly the answer is probably expert judgement. Until we get a lot more data, we still won't know much better.

Steve Gentili, Cathedral: But it is the road we've been forced down by regulators, which is, "you can model it to the 'n'th degree" without possibly truly understanding it.

Emma Watkins, WR Berkley: Yes, it's to parameterise something that you don't really think is possible to parameterise.

Matt Harrison, Hiscox: Maybe, but you still need to be able to define the bet you're taking. You need to be able to say to the interested parties in your organisation, that, in the event of a massive cyber attack your worst case loss scenario is X.

Emma Watkins, WR Berkley: Absolutely. That's the important thing. You want to know that if the worst thing in the world happens you are not going to go out of business. But saying there's a 0.5% probability of that happening, that's the really tricky bit.

Suki Basi, Russell Group: That's being on top of the aggregate as opposed to actually pricing business, isn't it?

Matt Harrison, Hiscox: Yes, I think so. With any risk it's hard to price for the tail risk, that is the really large, highly correlated large losses, as by definition these happen infrequently.

Steve Gentili, Cathedral: But do you think it's such a tail risk? If the loss you mentioned at the start Peter, was several hundred million (cyber losses) per year, that would equate to a pretty big wind storm, which we would all know about. But it seems like there's a lot of sideways losses at the moment, aggregating up to potentially enormous amounts, so actually, your one in 20 could be more important, from a cyber perspective, because it's just an accumulation of attritional net losses.

Matt Harrison, Hiscox: At the moment a lot of it probably isn't insured, and some of it is actually insurable. Everything can be insurable, but whether it is currently at the moment, or whether the actual, original client thinks that that coverage in the first place is reasonable, because what you might want to charge for that kind of volatility.

Peter Birks: In certain areas the buyer and the seller cannot ever meet on price.

Matt Harrison, Hiscox: But they probably will, if this, you know, in another ten years. It's like most of these things, you get the evolution of insurance, because you have an evolution of claims and you believe that the regulatory framework will work.

Emma Watkins, WR Berkley: It was kind of surprising after 9/11 that people managed to price Terrorism insurance contracts. It was really "finger in the air", wasn't it? And then everyone starts measuring risks against an "average" risk, which cost about X online for some terrorism cover, and is it a better risk or a worse risk? So now, 13 years later, there's a whole market for it, and it all started with some numbers that were just "finger in the air" kind of stuff, because nobody really knew what the probability of something happening was. You are probably starting with that sort of thing happening on the cyber pricing, and in 20 years' time there'll be a big cyber market out there, and we'll all think we know what we're doing. But actually it will have been based on people who just said, "tell you what, I reckon I can sell some insurance coverage. It probably won't happen, so I'm going to sell it for five online".

Graham Clark, Liberty: But isn't that the fundamental pricing in the market? It doesn't matter what the market is, it's the same thing. At some point there'll be a market correction, and there'll be some losers from that. But there's always, hopefully, the companies that don't go bust, taking on the people insured by the companies that quit the sector.

Matt Harrison, Hiscox: That's almost a definition of a specialty market, isn't it?

David Singh, Amlin: The other thing is that when we look at terrorism, the counterterrorism measures are quite well understood. Counter cyber terrorism measures, they're not really well understood. So therefore, I know we're being attacked pretty much every single day, but actually, what are our systems? How far developed are they? What is a cyber terrorism event? And you've got so many different types of events that could potentially occur, loss of data, hacking, etc. We don't know that much about it.

Peter Birks: It seems to be moving towards almost an area of wordings.

Suki Basi, Russell Group: Wording is one, and also, I think if you look at the surveillance aspect of counter effects, I think some of these lines actually understanding the underlying buyer's capability of monitoring exposure themselves, because they're the ones that are buying it. So you want to differentiate those that have actually got good systems in place and protocols in place, from those that haven't. You say that, but if you speak to a property underwriter he would differentiate between the door that's got a lock and a door that hasn't.

Sian Fleming, Talbot: Well, comparing it back to CBI. When you look at CBI, the people who have good risk management and know where all their suppliers are, don't need really need CBI insurance as they will have backup plans in the case of an event. It's the ones that don't have that in place who need CBI cover. And it's going to be similar with cyber. Those that have these excessive security measures and everything else, are less likely to need the insurance. It's the ones that don't, that don't have anything around them which is the risk, who will want it and need it.

Peter Birks: So you're saying there's a major selective bias in CBI and that really the only people who are coming in to try and buy it are those with poor systems in place?

Sian Fleming, Talbot: Not necessarily, but if you've got a really good risk management department, and you know where all your suppliers are, and you've got things in place for it if one of those goes down, you can switch when an event occurs that impacts you. If you have that in place, then how great is your need for CBI insurance? It's potentially going to be similar with cyber.

Graham Clark, Liberty: And then there's contagion, Sian (Fleming) mentioned the fire possibility. What about the other lines of business we write? So if we're looking at one in 250-year event, what is a one in 250-year event? Terrorist cyber attack? And is that literally the entire banking network of the UK going down? Then we're going to have some riots, and we're going to pay out our political risks, and perhaps we can't even get the train to work because all the train drivers are on strike because they haven't been paid. I don't know. What is the real connection? How do you even try to map that through? I think this is one of the biggest difficulties for large companies. ●