AGENDA JOINT APPG MEETING BUSINESS RESLIENCE AND CYBER SECURITY
31ST January 2023 Committee Room 18 3.30 p.m.

1) Chairmen's welcome: Ben Everitt MP and Simon Fell MP
2) Apologies for absence: Admiral Lord West, Jo Gideon MP
3) Present: Simon Fell MP and Ben Everitt MP (Joint Chairs), Baroness Neville Jones, Baroness Uddin, Lord Mackenzie, Rt Hon Sir George Howarth MP
4) Speakers:
    a) Tim Thornhill is Tysers' director of entertainment and sports.

    He was awarded the Insurance Insider Young Broker of The Year 2021 and Lloyd's and London Market Brooking Team of the year (2020 and 2021) prizes. Tim was heavily involved in working with the Government during the Pandemic in support of the Live Events sector.

    Here to highlight what Lloyds of London can do but also look at the shortfalls in levels of take up of cyber insurance in the UK. Less than 10% of the client base of Tysers have taken up coverage for example. Believes that there is further opportunity for engagement between Lloyds and Government.

    b) Toby Clowes is Tysers' Director and Head of Cyber Insurance.

    Been in cyber insurance for ten years since graduating. New area of coverage then, ill understood and somewhat of a luxury. Marketplace has been around for 25 years, based on the development of the Internet. Cyber security is now much more in the media and relevant.

    Began with US clients who were afraid of litigation. Have seen a shift in geographies and size of client from SMEs to multinationals. People are not going to buy a product which they do not understand this is key. Also key is the fact that the insurance market is reactionary, following trends.

    From 2017, we have seen that Cyber criminals are no longer hunting data but extortion. Education and knowledge are key and whilst the market has to be profitable it also has to be affordable. There has been a 4000% rise in losses.

    UK business is not well-covered and is cost driven to an extent but also a matter of education. It is the thing that is most likely to effect you financially if you read the Press.

    c) Patrick Davison, Underwriting Director at the LMA

    Oversees the technical underwriting and underwriting strategy teams focussed on supporting the managing agent underwriting community. The LMA Underwriting Team works in support of underwriting excellence in the Lloyd's market. This core function ranges from model wordings development to research and consensus-building in complex areas that are of concern to the market.

    90 syndicates operate on Lloyds, LMA is the trade association.

    Systemic exposure which the market faces is the biggest issue for the LMA. Experienced by buyers as exclusive language in insurance products. Cybersecurity insurance is unlike other markets as risks and exposures are constantly changing. Try to position the market at a sustainable level but knowing that the answers which we come up are not the correct ones. Is encouraging people to come up with innovative products rather than taking away coverage.

d) Neil Arklie is Head of Cyber Underwriting responsible for the oversight of the cyber (re)insurance market within Lloyd's.

Neil has been an underwriter for over 30 years and has been underwriting cyber for 20 years. Before joining Lloyd's he worked at Swiss Re, Chubb and Axis.

Cyber (re)insurance market is the fastest growing class within the Lloyd's market with Lloyd's underwriting approximately 20% of global premiums through 60+ syndicates. Lloyd's have been writing cyber business since 1999 and Lloyd's remain committed to this class but are aware it has unique challenge. Lloyds support Managing Agents who are experts and can create a resilient market over the long term.

Cyber insurance is supported by specialist law firms, cyber security firms and developing insurtechs who come to London for critical mass. Most insurance markets follow global GDP. Cyber has grown at 20% in the past.

UK has some special features: UK military, GCHQ, 5 eyes membership.

Looking for UK Govt to support the cyber insurance and security businesses and help us all through the challenges. Understanding cyber is hard as is mapping it. Hard to get customers to buy it so it would be great to use schemes like Cyber Essentials to encourage people to buy cybersecurity policies. It is more difficult to get cyber insurance as you have to go through various controls which improve your security.

Lloyds fall within a number of different HMG Departmental responsibilities: DCMS; Treasury (regulatory) and Home Office. Often the only people who can help clients who have a ransom attack as insurers provide the relevant help services. Request is that HMG recognises the unique opportunity for the UK.

Talent and training are a challenge, there is a national shortage of cyber professionals. Needed not only for breach response but also to work in insurance.

5) Open discussion and questions

Lord Mackenzie – I understand that the financial markets in London are ahead of the curve in terms of economic success. Does that include the insurance sector and particularly the cyber one?

NA – 90% of premiums are from overseas so we are contributing to the balance of payments. Also we have a unique eco-system for clients. The market divides up as 50% US, 10% UK and ROW is 40% and growing.

TC – growth is exponential. Characterised by brokers working together to share knowledge. This shows that the London market can respond to demands quickly but do need broking and legal talent. Other countries do not allow such a quick process.

Dame Pauline Neville-Jones – Lords/Commons Committee took evidence on ransomware. Heard that the take up of insurance is greater in the US than the UK. What are the US authorities doing that you would like the UK ones to do in order to encourage take up?

TC – US has a class action mentality which we do not have here, this drives insurance. In the US you have to notify the victims in writing if there is a loss of personal data. Not sure if we want to replicate this in the

UK. Businesses need to know that there are consequences if businesses lose data. GDPR has not been tested yet.

NA – GDPR has not had the impact that people expected. People buy fire insurance for instance because the bank has requested it to protect their assets. Challenge for the industry is to make it a product which people understand. Need to put cyber insurance into the same category as fire and theft policies.

Bill Mew – tried to bring cases in the UK, there is collective redress but the case law (Lloyd vs Google) followed by a ruling against DSJ means that a case can only be bought collectively at the County Court. Costs cannot be reclaimed which stops people from bringing a case.

Baroness Uddin – are you asking Govt to mandate insurance? Seems we do need to find alternative ways of working. How do you educate the public and companies so that they take preventative measures?

NA – would be good for banks and other lenders to see cyber insurance as a way of protecting assets. Seems strange that people accept losses through cyber theft but not their biggest exposure which is cyber.

US take-up is higher because the product is more mature. Not top of mind though, long buying cycle and it would be nice to have a nudge to push the market along. Insurance gives you indemnity for losses and access to expert help if a breach happens.

Baroness Uddin – are there any Universities which are working to meet the cyber security, Web 3.0 skills gap?

NA – Looking to partner with UCL, would like to invest in this.

Anu Khurmi – education and training is key for us. Partnered with a UK university to promote cyber research. Have launched a cyber MBA with Bangor University. It is an evolving environment. Need to help companies perform a proper risk assessment so that they understand what they are insuring against. Templar Executives links up with business people as well so the students have access to real experience in this field. Education is more and more important.

Dame Neville Jones – is the cost a problem?

TC – it is a marketplace, prices chop and change and react according to the losses. Five years ago the assumption was a catastrophic loss would happen once in a 100 years. Due to ransomware claims profit becomes harder to find in the insurance business combined with more aggressive pricing that lowered prices. Premiums jumped hugely to deal with claims. It is now levelling off. Seen as a luxury purchase. Also many entities do not update their security, need to get people to understand that insurance is a back-up.

NA – average premium was £1000 a year for SMEs. TC dealt with large companies with large losses.

Sheema Khan – as buildings need certain requirements to be insured, do you include somethings such as skills, expertise etc. as necessary for a policy?

Simon Fell MP – if I buy house insurance, there are conditions on that policy. What does that look like for an SME or large corporate? Secondly how do you score risk?

TC – large corporates: we look at loss trends over the last two years and look at what mitigates that risk (sandboxing, training, multi-factor authentication) and have tools that we like to see people using. We

also like customers to hold back-ups offline and to segregate data. In the absence of those, you are not insurable. We have seen the level of standards increase.

SF – what happens if the attack vector changes?

TC – the policy is for a year and we do not change it.

NA – SMEs are different. Can do it by way of mandating conditions, need to do basic cyber hygiene. If you don't put the lock on the door you will have a loss, not if but when. SMEs are more commoditised in terms of products used and policies offered.

TC – seeing rise of insurtechs who are reshaping the market. They are making the market more proactive. They might scan an SME to make suggestions and update this regularly to alert the SME to the vulnerability. They can advise SMEs what to do. They tend to be priced very cheaply and help at least some better themselves.

Durgan Cooper – interested to hear that you only have 10% uptake. You cannot mandate insurance but with the majority of small firms being micro, the more mandation from wherever would be better. Cyber Essentials for instance would assist if mandated as it is in some areas.

NA – It would help UK plc

Ash Hunt – Buyer of cyber insurance for the past 8 years, the product causes the lack of uptake, there is little ROI in it. Do not claim for most of the losses that are incurred as these cause higher premiums. Also finds a lot of misunderstanding in use of terms. Hard to correlate which vulnerabilities will be exploited and which not. 90% of loss is by accident not by ransomware. Market struggles as insurance is not attractive.

NA – no-one sees value in insurance until you have a loss. As a market we need to mature so that we respond to your [asset manager] needs and also to the baker's down the road. The market is still small in relative terms so not responding to your needs is not a surprise. Product is too homogeneous at the moment but it is evolving.

TC – there are, in London, 40 different policy forms which use different terminology. The ultimate scenario is that businesses work with a broker who knows them inside out. For the SMEs this is going to be harder and harder.

NA – more use of Cyber Essentials would be better.

Bill Mew – concern is in the mid-market. We see inadequate schemes due to fluctuations in risks and also numerous exclusions that are applied to policies. Concerned that there is an inadequate ability to price risk, look at risk rating for buildings!

NA – midmarket is an area where a lot of claims have been paid. Need more tech and assessment to make things work. There are going to be exclusions in a policy which should be explained and accepted by the client. We do a lot of stress testing at Lloyds and have a large team that look at capitalisation of syndicates to ensure that they can pay out if needs be. We are continuously checking the marketplace and ensuring that it can withstand a loss.

AGENDA JOINT APPG MEETING BUSINESS RESLIENCE AND CYBER SECURITY
31ST January 2023 Committee Room 18 3.30 p.m.

Tim Rawlins – interested in exclusions such as State authorised attacks. Who takes the decision on the origin of the attack.

NA – have discussed this extensively. The reason that we have a problem is that war risks, which these are, cannot be covered by the market. It is not easy to work out but the burden of proof is on the insurer to prove this. The Insurance Market is capitalised at £2 Trillion and G7 spent many times more on Covid. We need to ensure that the cyber policy explains clearly what it offers. As the market expands this will have an effect on market cap. and will need to explain.

Tapping into Pool Reinsurance [PoolRe] is a route that is being explored.

Andrew Churchill – last year the City Corporation and Zurich stated that cyber is uninsurable. How do we work with this viewpoint?

PD – not impossible to ensure war loss, there is a War market. The issue that it faces is that it has to underwrite very cautiously. This is an emerging marketplace and we should give it the opportunity to respond. There is a loss that we cannot cover, not sure what the answer is. It maybe PoolRe. Cyber is not geographically limited like terrorism for instance. We need to have the conversation.

Anu Khurmi – Carrot and stick approach, if one is consistent in applying good practice would this benefit the client? Are no claims bonuses common in cyber insurance?

TC – have put no claims bonuses into policies. Premiums are likely to come down as claims are dropping off. Can see a reward but will see premiums peak and trough.

No Claims Bonuses are something used to win people over.

Lord Mackenzie – do you get many fraudulent claims?

TC – No.

NA – there is so much data that you can analyse, it is difficult to commit fraud.

Mark Sutcliffe –from the maritime sector. Members state the shareholders need to be aware of cyber issues so that they insist that the management takes out a policy. That is how to get a take-up in insurance, certainly in shipping. How do you share breaking cyber activities?

TT – this is our ask to pull together a group to share information at the right level so that threat level awareness is there.

NA – many insurance companies have internal threat intelligence people and they are good. They should share their knowledge with their clients. Maritime buyers have a very low penetration rate.

Dame Pauline – don't you as insurers have the power to convene such a group?

NA – this is being done, for instance some firms have apps to share information. We do not see future intelligence though.

Tim Rawlins – on the 40 forms, we still have not seen clarity on that question set. We find it hard to advise clients on how the insurer is measuring cyber threats.

AGENDA JOINT APPG MEETING BUSINESS RESLIENCE AND CYBER SECURITY
31ST January 2023 Committee Room 18 3.30 p.m.

TC – always changing. Forms are only as good as the day on which they were written. Insurtech has a lot of promise as they can keep you up to speed and assess insurance. You want a competitive marketplace which we have offering premiums. There will always be a breaking point.

NA – to have one standard is not good for something that is always evolving. We are not asking people to meet a single standard. Mandating is hard as we need to comply with competition law.

Ash Hunt – do organisations have enough maturity internally to measure risk and if not what could they do better?

Many use traffic light scoring, finger in the air guesswork. Is there a space for us to gain education for you to measure risk internally.

Everyone today has spoken about sharing threat intelligence. Most incidents are accidental, if a service provider drops out for some time we would claim. Are claims adversarial?

TC – always easier for the larger insurers to look at this. The information sharing structure helps them to share risk. We know in the US there is a lot of peer-to-peer sharing. Hope to see the UK going this way as well. 15% of claims are accidental, not adversarial. Insurance market offers coverage against systems going down for all reasons not just adversarial.

NA – parametric triggers are coming in such as Cloud downtime. Cyber market is very homogenous but will break the exposures down.

Bill Mew – not just downtime in Cloud. Seen AWS and Azure have started to use AI to do risk-based analysis of individual clients based on their usage. OVH Cloud had a massive fire in a data centre and this showed many clients what the SLAs are. Many had assumed that their data was backed up elsewhere.

TC – agree, if you can understand the vulnerability this is key. These organisations are open to data sharing.

Robin Oldham – going back to car insurance, is there a model where the cost is split between two parties such as when you have a crash?

NA – SLAs on these policies are tight and in their favour.

Ash Hunt – had a recent discussion with other CISOs and sanitising the claims data would be useful so that we could work out how it was doing. Very hard to find out.

TC – are people willing to share loss data?

NA – no, working with the market to at least anonymise data to make it meaningful. Would love to do it but a challenge.

Mark Sutcliffe – disagrees, in maritime, like aviation and banking, there is an appetite for anonymous data sharing.

Bill Mew – ORX provides a model for exchanging data.

Anu Khurmi – there is a precedent for information sharing such as the ISACs. There are also CERTs and the larger banks do provide resource and knowledge as well as NCSC.

AGENDA JOINT APPG MEETING BUSINESS RESLIENCE AND CYBER SECURITY
31ST January 2023 Committee Room 18 3.30 p.m.

6) Conclusions

On data the more that we can get better the product. Chair thanked the expertise in the audience and summed up the speakers. The meeting understands that the threat is changing all the time with both State actors and organised crime playing a part. The asks that have come out are:

1) More of a partnership approach with HMG to encourage understanding of cyber risk;
2) Help with educating people and raising the level of talent through qualifications in the UK.
3) Greater sharing of data about cyber attacks.