The future of Cyber Underwriting transcript

SOFIA GERAGHTY: We go now to speak on the future of cyber underwriting. I'm joined by Stephen Ridley, head of Cyber at Aviva. So, Stephen, you joined the cyber market or first started looking at cyber I think around 2010, a lot has changed I think in cyber since then and in the world more broadly, have you seen the cyber threat shift from that time to now, 2022?

STEPHEN RIDLEY: So the fundamentals of the types of risk that companies face are broadly similar now to what they were when I very first started. So, take for example ransomware, the hot topic of the last couple of years, especially, but a risk that's been around since the last '80s when viruses were sent out on a floppy disk and you had to send a cheque to a PO Box. And over the last 20 or so years that's changed massively from going the turn of the 2010s when bitcoin comes around into a much more mass market approach, a stack it high, sell it cheap model, target lots of companies but very low value and pretty easy to defend against. But then in more recent years, these much more big game hunting attacks or data alongside it and threatening to publish and ransomware as a service where big groups are able to sell their services to smaller less sophisticated gangs, that massively changed the picture from that side of things. But the fundamentals of that individual risk are still broadly the same now as they were back then.

SOFIA GERAGHTY: Well, it's interesting you say it on ransomware, because I think we all, I mean I definitely in my head maybe feel like ransomware was just invented in like 2018 or whenever it was, so it's interesting for you to actually say this has been going on a lot longer.

STEPHEN RIDLEY: Yes and it's one of those where people kind of see these big headlines. It's only really when you get the big events that it grabs people's attention. But there's been this low level activity for a long time and it's not really anything new. It's just that it's morphed; it's come to the fore. And it's one of the challenges really from an insurance perspective around this is it's the criminals that are the first ones to innovate and push into new ground with this. And whether that's from the insurance side of things, whether that's the security side, they're always the ones having to play catch up to that and respond and react to what the criminals are doing. Because there's no point us trying to get too far ahead of that, because if we do they'll just take a slightly different course and work into something else that gets around or circumvents what we're trying to defend against.

SOFIA GERAGHTY: And when it has been an issue I guess for longer, why is it, maybe, only the last I don't know like five to seven years maybe potentially, you know, better than myself, the market's been talking about cyber, is it because the risk has sort of gone up or is it just an awareness, I mean were there losses coming around before then, can you speak a bit on that?

STEPHEN RIDLEY: Yes so the losses have definitely been around for a long time before that, but it's been in a very different way. Like I said it's, what we've seen over the last few years, it's this changing tack from the criminal. So whereas before they were just targeting lots of companies, really small value, now we're seeing it being done in a much more damaging and detrimental way where it's not just a case of do rapid fire, hit as many companies as you can and just hope that people click on a link or open the file and launch it. Now criminals are spending a bit more time getting into a network, surveying what's in there once they're there, seeing what data they can take out and then deploying the ransomware as their final hurrah so to speak. And then that changes the picture altogether.
So, although it's the same kind of ultimate threat, it's still ransomware, the whole kind of process around it is very different now to what it was even three, four years ago. And that's played a big part in shifting the market as we've seen over the last couple of years.

SOFIA GERAGHTY: And most people, and you sort of mention there, we see these headlines, sort of held to ransom, you know, millions and millions of dollars or pounds, sort of like really low frequency kind of like very high impact events. From the insurer point of view, is that generally what it actually looks like, is it kind of then very low frequency, kind of high cost events, or is it more I guess nuanced or different to that?

STEPHEN RIDLEY: Right so one of the challenges for the industry at the moment, and again part of the reason why we're seeing such hard market conditions over the last couple of years, is that it has both elements. So it has the high frequency, low severity incidents, typically more your business email compromise type claims where you might have a very small amount of damage or it's a small fraud that's perpetrated on the backend of things. But then equally you have these singular kind of large loss events from ransomware typically would be the higher severity incidents, but then we also have the cat risk or the catastrophe risk attaching to it, where there's still this chance of there being an incident that affects hundreds, thousands, potentially millions of companies all at the same time, which we haven't really seen yet from an insured basis.
So we've had a number of near misses over the past couple of years with the likes of Kaseya, with Log4j, with Microsoft Exchange last year, all of which had the potential to be this type of big systemic event but hasn't quite come to pass as yet. So insurers are now very mindful of the risk that that could happen and having to make sure that pricing adequately reflects that as well.

SOFIA GERAGHTY: So we're seeing maybe recently as a result of some of the fear around cyber that there's lots of questions I guess for the end client. So if you're getting a picture of the client's cyber risk, then a lot of brokers they have to get all this information and it could be quite a sort of arduous difficult process to get all that information. Is that a long-term thing or do you think there's going to be more solutions to that?

STEPHEN RIDLEY: So it's definitely an area where as an underwriting community we need to do better. Like at the minute some new incident happened and every insurer compiles their own list of questions that relate to how that's been handled or how it's not going to happen again for that company. And it's just not a very customer-centric approach. We can't continue doing that for every new incident that comes around. So there has to be a better way of doing this. So for me there's an element around just understanding the customer themselves. Kind of focusing on kind of what are the, or to start with what are absolute fundamentals, you have the red lines that absolutely have to be in place for you as a business to consider underwriting that class of business, and that can be kind of the real objective measures, is this in place or is it not? And just red lines around if this isn't in place, not one for us. Then there's the other, slightly harder the gauge, but it's more around the attitude, the ethos of the insured around how they manage risk.
So, if we consider these incidents that I've already mentioned around like Microsoft Exchange, Log4j, rather than asking pointed questions about each one of those, it all basically comes down to patch management and how the business deals with assessing new vulnerabilities as and when they're released, working out what their impact might or might not be, how they might be affected by those, how they go about remediating those. Getting the idea of how well prepared a business is to go through that process, should give you comfort that if they can manage one type of these incidents then that should carry forward on to the others. So understanding that there are the right controls and processes in place is much more important for me rather than picking individual items, because you can look at any one of those incidents and a business might not have any exposure to it whatsoever.
So asking the whole host of questions doesn't, about that one event, doesn't really get you any further forward, rather than considering OK, if there were to be this type of event, how would you manage that, how would you ensure that patches are applied in the most appropriate timeframe based on the sensitivity of the vulnerability things such as that.

SOFIA GERAGHTY: OK. So rather than looking at individual systems, it's more about the management process almost of the company.

STEPHEN RIDLEY: Yes that's right.

SOFIA GERAGHTY: And so if I was a broker, you know, you imagine brokers do have targets and things like that, and cyber, you know, it's all this new information sort of you have to learn, it's quite a difficult market, it might be easier let's say to sell like other lines of insurance potentially from the brokers maybe. I mean what would you say to brokers that kind of feel that way, would you say that cyber is still an attractive risk to be selling?

STEPHEN RIDLEY: For me, considering cyber as something that needs to be sold is almost where the problem starts. This isn't just selling a new or a bolt-on piece that is just a way of hitting targets and of generating extra money through premium or commission, whatever it is; this is a product line that has fundamental value. We heard in the panel session, previously, Will saying that the hard market conditions proves the value of this product. We're in this position because insurers have paid out tens, hundreds of millions of pounds worth of claims, which proves that there is a real need for this product. So it shouldn't be a case of just going out and selling it. The whole thing needs to flip on its head really and it being about risk, understanding risks that businesses face, and many businesses now, if not most businesses, cyber is going to be the most critical fundamental risk that they face as a business. It's not a fire in their office, it's not an employee slipping over at work; it's their systems being rendered unavailable due to a cyber incident.
So it just needs a slightly different mindset, a different approach, a consideration of risks. So rather than it being a case of have you considered this new policy that you don't buy yet, taking a step back and saying what as a business are the critical risks that you face and how can we make sure that your insurance programme completely tailors to those risks.

SOFIA GERAGHTY: So I recently thought I want to improve my cyber knowledge and I found, it was only a quick search, it wasn't quite clear kind of how to do that, what qualification bodies and things like that, it's not like say like CII for example it's quite clear. When you're talking about understanding cyber, I mean how long does it take to actually become cyber literate and what does that process actually look like?

STEPHEN RIDLEY: One of the problems with cyber, and this isn't an insurance issue, this is a cyber field at large, is that there's no real consistency across the board, and as an insurance industry and through the ABI, through the IUA, we've been having conversations with government around how we can get more, a more homogenous use of terms and things such as that, how can we raise the bar in a consistent way across the board, how can we get rid of some of the complexity and the jarring of language between these, which doesn't help in the space. But the fundamentals are quite simple to understand and I guess it's easy enough for me to sit here as someone who's…

SOFIA GERAGHTY: A veteran I guess from 2010 if we look at the cyber market.

STEPHEN RIDLEY: But, equally, I don't have any god ordained gift in this space. I wasn't born an expert in cyber risk, nor were any of my peers. It's something that I've learnt. There's nothing special about me in that respect. So if I can do it, if any of my peers can do it, then there's no reason why anyone in the industry can't learn it. And you don't need to be an expert right down into the real detail of it. You don't need to know how to architect a network, how to configure a firewall, anything like that, it's all about fundamentals of risk, which the insurance broking community at large are absolutely expert in. Whether it's construction risk, whether it's property risk, whether it's liability risk, we have these experts all around the industry, and cyber is just a different peril, and understanding just some of the small nuances to it is relatively straightforward.

SOFIA GERAGHTY: So I mean what is the first, if you're a broker and you're like OK I want to upskill, I do want to start adding, in terms of education what's the first step really would you do?

STEPHEN RIDLEY: So I'd just be trying to read things. So there's lots of free resource online, the NCSC website is…

SOFIA GERAGHTY: National government.

STEPHEN RIDLEY: Yes National Cyber Security Centre is an excellent source of resource. They've got some pretty high level reviews on there that are free, easily accessible, which can just tell you some of the basics or the real kind of critical things to be looking at. Or considering things such as cyber essentials accreditation process, just looking at what are the areas that that focuses on, because that is a scheme that's designed to eradicate that 80-plus percent of the risk. So if you can understand just some of those basic measures that they're encouraging businesses towards, you get a feel for where things are heading. Lots of the security companies have blogs and things like that, that can get slightly more into the technical

detail. But also speak to underwriters that you know. Kind of I know we at Aviva do lots of training courses for our brokers and we can pitch those at a really basic level, an intro as to around cyber risk itself and how policies respond. So there's a whole wealth of resource out there that people can tap into.