PRESENTER: Here to talk about tailoring cyber cover to SMEs, I'm joined by Stephen Ridley, Head of Cyber at Aviva. Hi Stephen.

STEPHEN RIDLEY: Yeah.

PRESENTER: So my first question for you is obviously you've had the cost of living crisis and lots of businesses struggling, have we seen a decrease in the uptake of cyber insurance?

STEPHEN RIDLEY: So the cost of living crisis is, unquestionably, affecting everyone including most small businesses in the UK. But we haven't actually seen it manifest in terms of kind of a reduction in companies buying cover for the first time. It's still very low compared to what it should be. But we just undertook a pulse survey of businesses recently and only 2% said that the cost of living crisis had a direct impact on them making that purchase. But still almost 20% found that cyber insurance was too expensive for them to consider buying. So, where we're seeing premiums rise across the board, not just from a cyber perspective but general lines of business as well as claim inflation is starting to hit, then it's definitely making businesses think about whether they have the available budget to buy a new cover, which cyber generally is for most of them.

PRESENTER: So cost is a worry, but it's not necessarily down to the cost of living crisis.

STEPHEN RIDLEY: Correct, yeah.

PRESENTER: And you mentioned there that underinsurance is still high. I mean for cyber insurance, I don't know the exact figure but I know it is low compared to other types of insurance for businesses and things like that. I mean why is that?

STEPHEN RIDLEY: Yes so it's around 20% from our survey said that they buy specific cover, and expense is one of the big things that's listed. But then the next one is that small businesses still struggle to see cyber as being relevant for them. They think that they won't be the target of an attack or think that it doesn't fit kind of their business and how they operate. But actually we're now seeing that 50% of businesses say that they are more reliant on digital systems than they were pre-pandemic, and almost 20% are saying that they are wholly reliant on cloud technology. So this is real fundamental risk for businesses nowadays regardless of what size or industry they're in, and isn't something that can be put on the backburner continuously, it needs a slight shift in attitudes towards it.

PRESENTER: And with that I mean I guess what sort of can be done either, you know, from the insurance industry to kind of improve the take-up of cyber?

STEPHEN RIDLEY: I think there's still a big educational piece to do, in part to help combat this feeling that SMEs aren't vulnerable to these types of incidents, which just isn't the case. We see that 20% of businesses in this survey said that they had suffered an incident in the past year, which would be much higher than has had a fire or a burglary or any other type of incident. So this is now one of the most critical risks to these businesses. So it needs education to help realise that. But also education around the availability of cyber cover and how it protects, so we still see a huge number of businesses think that they have cover through other general lines of business. Which may well be the case, but I would hazard to guess that it's not likely to be the case in the vast majority of situations. And also we see about 10% thinking that they have cover via their MSP. And again may be the case in particular circumstances, but I'm not aware of anything or any arrangements such as that myself. So I imagine there is a bit of a misalignment of expectations on how the insurance policies will respond, so education is really front of mind with this.

PRESENTER: The sale of policy there, I mean is it generally with cyber that sort of the one size fits all or do we see sort of a lot of variation in the types of policy available?

STEPHEN RIDLEY: So what we see with most markets is there is an element of tailoring available, but what tends to happen is it's either an all or nothing approach, which means you either pay for the gold plated package or you take nothing at all, and that's often the two options that are presented to businesses. In part because of the complexity to the area or the lack of confidence that people have in discussing the topic, but actually there is a middle ground where you can tailor the cover to be more relevant to individual businesses within the suite that's available and get to something that's at a price point that then becomes accessible or palatable for that particular business. Whilst not necessarily covering absolutely every risk that they might face but covering the most pertinent ones for them.

PRESENTER: And do you feel like I guess cyber can be better tailored to clients, I mean is that an area that the industry could maybe improve on?

STEPHEN RIDLEY: So I think it can be made more accessible, yes, and part of that comes back to the education piece. It needs us as insurers to educate our brokers on the amount of tailoring that is possible and really explaining what the elements of cover do and how they can respond. And then it's the brokers to educate their clients on what those do, and also help to identify, you know, where are the biggest pain points of cover, what are the elements of cover that are most relevant for them,

and rather than buying your kind of highest limits across all of the elements of cover, actually would the business rather prioritise certain elements to make sure that they're best protected in the areas that are going to cause the most harm if that event happens.

PRESENTER: Yes there's I guess tailoring of things like the limit and the policy itself and then there's also maybe tailoring of the services they have access to which might differ from business to business.

STEPHEN RIDLEY: So the services I'd generally see staying fairly static that they have access to in terms of the claim response. But definitely the limits that they have and the actual sections of cover, the elements of cover that are available under the policy is definitely something that more could be done to tailor.

PRESENTER: And in terms of I guess understanding a business' risk profile itself and their exposure to cyber, what do you think are the best tools and kind of ways of doing this?

STEPHEN RIDLEY: So the proposal form is still the main tool that most businesses, most insurance companies will use to assess that risk, and they definitely have a part to play. But they are a very blunt instrument. They're that point in time view and they don't capture the shades of grey that might exist within it. It's very binary typically yes or no answers that you can capture. So what we're increasingly seeing companies doing is using external scanning technology. So the ability to look at what the external perimeter of a company's IT network looks like, see if there's any vulnerabilities or open ports that might be dangerous to that business, and use that to inform the underwriting. But it is just that, an informing process to it. It's not the be all and end all to it. Because you get a lot of false positives within it, but what it can be is a conversation starter. And actually what I personally find in the situations where you can do it is a conversation with the insured is by in a way the best way to understand both where their exposures lie but how well they're doing in mitigating those exposures.

PRESENTER: So conversations still is kind of a mixture of things by the sounds of it.

STEPHEN RIDLEY: Yes absolutely. There's no silver bullet to this. So you can't rely on any single one of those features, you still kind of need the blend of it, and part of the skill of an underwriter in this space is knowing kind of when to rely on one more than the other, and how to balance them out, how to take the information that's presented in those and hone in on what is the most important elements to understand a bit more.

PRESENTER: As I think you mentioned earlier I mean most businesses now, maybe not all of them but most of them have an online element or at least have a website or something like that. I mean what businesses are most at risk of attack?

STEPHEN RIDLEY: All of them is the long and short to this. So it's rare now that criminals or people who are looking to cause harm sit there and think I want to go after this particular company, this particular industry. Yes there will be some of that through targeted phishing campaigns, but the majority of it now is much as we as insurers do these scans of company networks, the criminals do the same. That's kind of how they gain their initial access generally. But they're not scanning individual companies. They're just looking for these common vulnerabilities, these common open ports. And whoever it is that's behind that, they'll look to gain access to that system. And then once they're in, figure out who is it, how much value can we extract from this particular business. If it's a smaller business, then it's more likely to be a really short simple lower value type of attack. But if it's a bigger business then they're more likely to spend more time understanding kind of that business extracting data from it, performing more of a sophisticated attack that is more likely to be really disruptive.

PRESENTER: So it's more kind of looking for businesses that are maybe more vulnerable in terms of cyber defence I mean.

STEPHEN RIDLEY: Correct yes. So those that have more externally visible, so those that are the lower handing fruit, those that haven't done the basics to keep their systems in check. So haven't patched, haven't applied patches in a timely manner, haven't made sure that any unnecessary ports are closed, haven't updated to the latest operating systems, things like that. Yes so criminals will always go after those easy targets.

PRESENTER: So, if we move now to training, because a lot of SMEs might have a smaller kind of staff and things like that, does everyone need to be trained when it comes to cyber?

STEPHEN RIDLEY: So I would say yes. Your training is one of the most simple, cheapest but most effective ways of avoiding these risks. The number of incidents that we still see that are caused by someone clicking on a link in an email or not checking payment details before sending or before changing bank details for one of their customers, these are all things that are quite simple to overcome. And training doesn't need to be a big burden. You know, for staff, it could be 20/30 minute session every few months. So it's really simple to get through and that can be really cost effective for a business to implement as well. Because ultimately humans are probably the weakest link in the chain as far as cybersecurity goes. So, for a relatively modest investment, it's a really

good way of improving the overall baseline of security, and it's one of the things that we do at Aviva is provide our customers with access via one of our partners to some online training, we have a preferential deal with them, so helping to make it even more accessible for them.

PRESENTER: Stephen, that's all we got time for, thank you so much for joining me today.

STEPHEN RIDLEY: Thanks for having me.

PRESENTER: And thank you for watching.

END OF RECORDING