Insure TV Masterclass : Cyber innovation transcript

MARK COLEGATE: Hello and welcome to this Insure TV Masterclass with me, Mark Colegate. We are looking at innovation in the cyber market. To discuss that, I am joined here in the studio by Stephen Ridley, Head of Cyber at Aviva, and by Tom Draper, Head of Insurance UK at Coalition. Those are our panellists. Let's get things straight underway.

Stephen, we're talking about innovation,why is that so important in the cyber market, particularly from Aviva's perspective?

STEPHEN RIDLEY: So I think there's probably no other market where innovation is as important as in the cyber market, because we're not dealing with a stable risk, it's a risk that is constantly evolving. And in large part because it's a man-made risk, there's people on the other end of this. And what we tend to find in this space is that criminals are the main innovators and early adopters of new technology and ways of doing things. So we always need to make sure that we're keeping pace with that. We can't rest on our laurels and just treat this risk in the same way that we have done for the last five, ten, twenty years. There's a need to constantly be pushing what we're doing, making sure that not just the product itself from a policy wording standpoint evolves but the way that we underwrite the claim response that we provide within that, the value-add that we provide to customers within this always needs to keep pace. We've seen over the last few years as ransomware has evolved from being a stack it high,sell it cheap model, try and hit as many people as possible, criminals then pivot and evolve and innovate and start extracting data, which adds extra leverage,and that was a real big game-changer for the insurance market and has led to the market conditions that we've seen over the last couple of years and has led the market to handle things in a very different way to what it did previously. And that's something that we can't just think OK we've been through that round of innovation, we can sit back and relax now, there will be another innovation, there will be another step forward. We're going to have to react and adjust accordingly. And that's something that we need to be constantly mindful of and is certainly how Aviva, I'm considering things and making sure that we're set up not just for now but for the next thing that happens.

MARK COLEGATE: Thank you. Tom, tell us a little bit about how you're seeing things from Coalition's perspective?

TOM DRAPER: Yes, I think from our perspective, while the cyber market and insurance policieshave existed since 1997, 1998, I think when it comes to innovation, it's about how can we help brokers sell what for them is probably a new product, for many of the teams in the UK it's a new solution they've yet to present to clients, but also for many client they're viewing this risk as an insurable risk for one of the first times. So, when it comes to innovation, we have to rethink actually how can we help brokers support the clients, how can we explain the solution, but also adapt around the concerns that get raised by both the broker and the client for what is a new purchase.

MARK COLEGATE: And how much of this, Tom, is because we all trust the internet? I'm old enough to remember back in the day where people said I'll never put my credit card details into that, you've no idea what's going on behind the scenes, and about the point everybody says ah we feel completely comfortable putting our data on, is about the time suddenly people start to say hang on a second, there could be bad faith actors.

TOM DRAPER:
I think, yes, very much so, our comfort levels with the internet, but also our comfort levels

with technology. We've seen a large change in the last three years of the ability for firms to work remotely via large scale networks to support their customer base. And as a consequence that's also changed the risk. So, while we've got more comfortable with it in our own personal life, we've also become aware from a business perspective how much we rely on our systems,our to our cyber-exposed assets.

MARK COLEGATE: Stephen, you're talking about this innovation particularly from the angle of it being driven by bad faith actor if you like. So what happens if I've got an Aviva policy and a whole new different type of risk appears six months into my policy and I get hit as a result of it? I'm the victim of innovation over quite a short time period. Are you likely to pay out on that, assuming you haven't done anything wrong? I just want to get a sense of how comfortable you are buying a policy and then when you need it, it's not there to help you in the small print.

STEPHEN RIDLEY: Yes. So, absolutely, I would expect that to be covered by the policy, obviously all the full terms and conditions and everything, but where we've put a lot of focus and emphasis on making sure that the policy is set up in such a way that it can cater for that additional innovation that might come, not being too prescriptive about what we're providing under the policy itself so that it only covers what we're seeing now, making sure that those terms are written in such a broad manner that they can deal with that next step, that next iteration, that next innovation that people can come up with and with our incident response partners, with the people who are on the ground handling the claims, we're constantly keeping an eye on what is going on, how might we need to adjust our claims handling response, what are we starting to see happen. So we're now considering things such as 5G, which we're not necessarily seeing at the moment being a big pressing issue, but it is a next logical step that might become an issue down the track. So how do we make sure that we have the right bits and pieces in place so that we're not scrambling around at the point at which there is an issue. We already have some of that legwork done ahead of time. We're trying to pre-innovate almost.

MARK COLEGATE: On that, Tom, would you agree that perhaps a bit of fuzziness in terms and conditions is there to protect the policyholder rather than to give the insurance provider a get out of jail free card?

TOM DRAPER: I think there's very much a focus on outcome-based in our policies, which is very much what is the consequence to the business; not necessarily what causes it, it's what's the impact to the business? You've had data compromised, you can't access your systems,you've lost information and you're now being investigated by a regulator. However that's caused on the front end, that's really or us, as insurers, to mitigate the price and underwrite effectively. Actually from a customer perspective,we need to support them no matter what the cause is.

MARK COLEGATE: And just in the round, before we really dig into the detail of this, how big would you say the protection gap is in the UK today? Tom, is there a figure you can put on that? Then I'll bring Stephen in on this.

TOM DRAPER: I think it's very interesting. At Coalition, we apply our own metrics to every single client and prospect that we see. We are definitely seeing a difference between the maturity levels in the US for SMEs compared to the UK. I think that's driven by two factors: one, the US, there is more of an established cyber insurance market who have been pushing higher standards for a number of years, but also the wa the US government has supported SMEs compared to the UK so that's something that we'll be definitely releasing more information on as we think there are key changes they can make for UK.

MARK COLEGATE: OK, thanks, so without putting a number on it, the UK feels behind on the US. Stephen, can you put a number on it?

STEPHEN RIDLEY:I think it's huge, is the short answer to that. The volume of customers that are buying a specific cyber insurance policy is just tiny. And I think there's always a massive overestimation by customers as well about what cover they do have. I was at the BIBA Conference last week and almost every conversation that I had with brokers, I was asking them exactly this point, how many of your customers buy a cyber policy? Not one of them said more than 10% when we were talking about that, so that's 90% of companies not buying cover at all, and then of those that do, there's likely to be a protection gap in terms of are they buying a limit that is sufficient for their needs. But what we see in a lot of the government surveys and things such as that is that number of companies that say they're buying cover is more like 20 to 40%, so we've potentially got 20% to 30% of companies that think they have some form of cover where they may well not, and they're existing in this belief that they have protection, whether that's within other existing non-cyber policies that they buy, whether it's their managed service provider that's providing some kind of element of cover, we see all of these different myths out there or misbeliefs that people might have.So there's a real need on the insurance industry or us as insurers and brokers to be better educating businesses about what the risks are to them, but also how they can best protect themselves against those risks, what are the limitations of those non-specific policies that they're buying and what is the true value of a full specific cyber policy, which is an immense value.

MARK COLEGATE: But how do you overcome that, because, just going back to something we were saying a bit earlier and Tom was saying is, data and the internet is everywhere and therefore I can see why somebody's first reaction would be well yeah but I'm sure it's covered by something else because I've layered all the other insurance policies in every other aspect of my business, I've just moved some of it online, it's covered by that?

STEPHEN RIDLEY: Yes, and I think education is then back to the key around that. I think it's a word that we've both used already today and for me is the most critical part of what we need to do around this. It is providing that education, that assistance, both, to start with, from our standpoint, to Aviva's brokers and then helping them to educate their customers as well on the back of that as to how is the best way of protecting against this risk.

MARK COLEGATE: Tom, when you look at cyber, what are the pros and cons, as a provider, of targeting large firms, which I guess we all seein the headlines when something goes wrong, versus this huge range of SMEs that are out there is it efficient to do it?

TOM DRAPER: I think, from our perspective, we've been focused on writing SMEs since we started back in 2017. Our belief there was very much an area that wasn't supporte by predominantly governments and also the security enterprise firms at the time. So we were fulfilling a need that needed to be supported. I think especially all size companies have the same problems. They all have a resource challenge. They all view cyber as you've raised earlier, as a bit of a tough risk to get their hands around. I think the difference for SMEs is they just don't have the bandwidth, and that's why they're looking for more support.

MARK COLEGATE: And on that particular point, if you go to an SME, can you talk through anyone you've seen, a broker who's got a successful policy of being able to sell into it, because, from what you've both said, it sounds like a policy that needs to be sold rather than one that flies off the shelf by itself, so what are some of the successful tactics you've seen brokers use to explain what the risks are and why it makes sense for a client to use it?

TOM DRAPER: Certainly. I think the start point is for a broker to realise they don't need to be a cyber specialist.They don't need to be an IT tech or a security firm. They're operating as a risk adviser, because then it becomes a risk discussion. It's not about what tech do I have, it's what are you doing with your business, what protects you, what concerns you? And then that's where we, as insurers can then support brokers here's the data that we have, here are the concerns that we see, here's the risks that your clients are impacted by. But you're talking about it from that perspective, and what can help their business operate, less of a transactional perspective.

MARK COLEGATE: And what's the point that someone like yourself as Coalition would get involved in that, because I can see explain the risks in terms of what you've got around you in your business every day, but at some point you have to have a conversation about what those things are that can come through if you like the very real doors and walls in your building?

TOM DRAPER: And that's very much our role. So at Coalition we provide brokers with the information that they need to have a conversation about a client.They see the risks the client face from a security perspective, here are the concerns that we've seen, here are the exposures, here's what we think a loss would look like unique to that individual client and, more importantly, here's support around you to get yourself better. So I think it's very much translating it into focusing on that specific client, what concerns them.

MARK COLEGATE: Stephen, what's the Aviva approach?

STEPHEN RIDLEY: Yes, and at the risk of being very boring, I completely agree with most of what Tom said there, where it's all about making this a risk-based thing. And I think one of the challenges or the barriers that I find brokers coming up against, is just trying to sell a cyber policy and saying that having a piece of paper and trying to sell the customer that without bringing to life what is the challenge that that business might face that that policy is helping to solve. And, for me, it's about dialling it back to what are the consequences that a business is most concerned about, what are the things that are going to cause them the most amount of pain? And in a world where we are now incredibly reliant on digital technologies, as we've already spoken about, it's that access to computer equipment, that access to networking. For most businesses now that is going to be the most critical risk that they face, or the loss of that connectivity is going to cause them a bigger issue than their building having a fire or being burgled. So if you can flip it round to be what are those main risks to your business and how can we go about best protecting against those risks, that's when the value of a cyber policy really comes to life. And that, to Tom's point again, is where we as insurers can come in and provide some of that supporting material around this is what that can look like when it goes wrong.

MARK COLEGATE: So it's more what happens if your CRM system disappeared or your entire payroll, what would you do?

STEPHEN RIDLEY: Yes, you get to your office on a Monday morning, none of the computers turn on, what next?

MARK COLEGATE: OK. Tom, are there any other, again you've both stressed that risk is evolving all the time, but within SMEs, are there particular, put it in those very concrete day-to-day terms, you've talked about things like CRM, payroll, computers don't turn on, are there other key things that make people think oh my goodness that definitely could happen to me?

TOM DRAPER: Well I think you touched on it there, which is reliance on key vendor partners. So for many large enterprises, many large risks, there are actually, there are many different vendors they use and many different IT providers they use. The challenge most small businesses face is if their main IT provider has a problem, that's their business. And they've rightly turned around to that provider and trusted them with their security, their information, their data, but that's a key reliance for them. And again I don't think many firms think about it in the same way that they would, oh we don't have access to this building. But actually if you don't have access to that system, that is a key problem, and that's one of the key reasons for purchase of a cyber policy.

MARK COLEGATE: OK. I suppose the other thing is, to what extent do you want to sell cyber policies in the SME space as standalone policies and to what extent can you wrap that into other existing business? So, Stephen, I'm sure as Aviva, you're a big brand, you must do a lot of insurance with small and medium-size enterprises around the UK, what would you?

STEPHEN RIDLEY: Yes, indeed we do. So we're the largest general insurer in the UK. So naturally we have a large base of existing customers in that space. So I think it's incumbent on us then as having that leading position across all other lines of business to take a leading position in supporting around cyber risk. And we can provide our cover as a standalone policy in its own right, but equally we can provide exactly the same cover as part of our wider commercial, combined or other packaged insurance policies. And one of the ways that we've innovated over the last couple of years is actually looking at how can we make that process a bit quicker, a bit slicker, a bit easier for our brokers. So where we're writing these other insurance policies, we already have a vast amount of information on those businesses. So we take that data. We supplement it with some other external data and apply some other factors to that, and we're then able to automatically generate cyber quotes on the back of that so that we can pre-arm our brokers with something as a conversation starter with their customers, where it's not just a, or faces off to that question of well how much is it going to cost? Straightaway, we can give them a bit of ammo to support that conversation.

MARK COLEGATE: So essentially if I say, my language not yours, cyberise your existing insurance, and say for another £200 a month you'd be covered for all of these other risks or, you know, you'd be properly covered for these risks, you think, or whatever happened to be.

STEPHEN RIDLEY: Yes, that's it. So based on the information that we have, we can provide you, subject to getting just clarification on a final couple of points, we can provide cover for x amount.

MARK COLEGATE: OK. And, Tom, how does Coalition go about doing it, because I guess you haven't quite got the same footprint as an Aviva, are you a specialist that likes to bolt-on to the side of other existing insurance covers from other providers?

TOM DRAPER: It always comes down with what's the easiest way for the distribution partner, what's the easiest way for the broker to talk to the client? I think the view we've always had is that a small amount of good cover is better than no cover, so actually how can we assist companies to do that? Our limits start at £25,000; we've got a £10m. We provide bolt-on solutions, standalone solutions. It's really what works to help the conversation, what is an easier part of the process for the broker to transfer that risk.

MARK COLEGATE: And once somebody has taken out cyber cover, whether it's with you or someone else, but once they're in the habit of doing it, what tends to happen in the journey, do they start off with not enough cover and they say that worked, and keep being underinsured for years and years and years, do they suddenly start to get quite into the nooks and crannies and what could go wrong and actually build their, you know, so when you look at it you think actually over time it's a four-year journey to being fully insured, what are some of the things that you're seeing?

TOM DRAPER: Yes, very much so. I think that's why it's actually a very attractive proposition for brokers.

This is very much a product that once a client has, they realise the value in. They're able to experience it, see what would be covered, they're able to see the applicability to their business, and, more importantly, the broker's able to have that conversation again at renewal, and here's claims that we're seeing, here's challenges that we're seeing, therefore you should look to increase the limits being purchased.So we very often see very low limits purchased year one,initial toe in the water, and then with the advice that we provide, the data we provide, brokers are far more confident to talk about actual real limits, more transferable risk at renewal.

MARK COLEGATE: Stephen?

STEPHEN RIDLEY: Yes, and it's definitely something that we see as well. And particularly as the risk evolves and that changes, so what is, even if the limit that was purchased two or three years ago was sufficient at the time, there's a risk that it might not be now. So having that constant process of reviewing and considering what the risk is and how can we buy the right limit to match up to that I think is a process that we see happening quite frequently. Especially now that we're getting through the backend of the hard market and starting to see slightly more favourable conditions, particularly around excess layers, actually we're seeing more and more companies extending the limits that they're buying.

MARK COLEGATE: When you look at your book of business at the moment, Stephen, there's lots of pretty small niche-y tech companies out there. Do they tend to be pretty good at buying cyber cover in the round, they understand the risk, or do they think we're geniuses in this space, that's for the peasantry?

STEPHEN RIDLEY: Yes, you tend to get a mix at polar ends of the spectrum, like you get those companies that really understand the risks, that are really concerned about it so buy the cover, and then you do get those that think oh yeah I know it all so I'm immune to this so I don't need to worry. But what we tend to see is that technology companies are probably the sector that buys cover most frequently, there's the highest penetration into that sector, largely due to contractual requirements, I imagine, rather than necessarily them seeing the risk better than other companies, but there is that element to it as well.

MARK COLEGATE: And, Tom, we're talking, our headline is innovation, but a lot of what you've been talking about is actually, it sounds to me, you're both describing a story that's much more gradual and much more evolution than revolution innovation. Am I putting thoughts into your head there or words into your mouth?

TOM DRAPER: I think that's accurate. As I said, the cyber market started writing policies in 1997. It is always going to be a continual evolution compared to the threats that we're facing, but also how clients respond to that and see how the market will develop. I think the biggest changes we've seen in the last two or three years has been the speed of the evolution, and that's definitely something at Coalition we're pushing, reaction to threats, how we can evolve around that and how we can support our clients.

MARK COLEGATE: Certainly at the moment we hear a lot about cost of living crisis, not just for individuals but for firms as well, and I think you alluded to that a little earlier, Tom, so what can you do as insurers to help brokers make the argument for, as you said, this, I won't call it a new type of insurance, but what might publicly be seen as another blinking policy to buy at a time when inflation is taking a real bite into the real value of what firms are earning, how much money they've got to play with?

TOM DRAPER: I think it's a very good time for brokers to be talking to clients about why they're buying any of their insurance policies. It actually needs a deep thought about what's their approach to risk, how they want to transfer it, and actually the realisation that over the last three years they have moved to a far more online remote based organisation that means their digital risk has increased, so now is actually the moment where is your biggest asset or threat your physical belongings that you have, your buildings, those type of assets, or is it actually more of your cyber exposures?

MARK COLEGATE: And in terms of bringing costs down, Stephen, are there any obvious things that you can do as an SME that reduces your risk and therefore means that you get better terms from Aviva or Coalition or anyone else, just because you've closed off, you've shut the obvious gates?

STEPHEN RIDLEY: The cyber insurance market has evolved, has matured a lot over the last couple of years. And that's not a maturity just from pushing the rates up and taking a closer look at things from an underwriting perspective. There's actually now a lot more data supporting what represents a good risk, what represents not such a good risk, and actually there are more favourable terms available for businesses who are able to evidence that they have a good strong security posture, particularly around particular elements of that risk, so whether that's things such as having multifactor authentication in place,having a good backup process in place, having completed something like Cyber Essentials. I know we give a discount to businesses that have gone through that process. I know many of our peers do as well. So going through that process is not only going to make you a better risk but also make the insurance slightly more affordable or you as well.

MARK COLEGATE: Thank you. Tom, what are your thoughts on I suppose preventative strategies, which I'm sure you would want to align with somebody having a policy, but what are some of the things you can do there?

TOM DRAPER: Very much so and that's very much how we approach our clients. We approach, look at clients the same way the attackers do. So therefore if the clients are more resilient they get a better price. There's a really good example for SMEs, encryption of portable media devices. That has a 15% load for us if you don't do that. Which means for any client, we can turn around and say by doing this, and there are many free solutions to do this, you save 15%, so please do so. The other aspect then is actually looking at what specific technologies they are using, and we're able to recommend which ones are more effective from a return on investment perspective.

MARK COLEGATE: And are there any good rule of thumb ratios, like for every pound you spend on cyber security you're going to save, I don't know, £50 on a three-year view, whatever it happens to be, are there any good rules of thumb that you've found brokers are able to use with clients that?

TOM DRAPER: I wouldn't have suggested so, because actually this is a risk that is not necessarily buy the most expensive piece of kit and it'll fix the problem; a lot of this is far more behaviour. It's about making sure you're doing the basic things right. Stephen mentioned Cyber Essentials, for example. That's a really good starting point from the UK government in terms of basic steps an SME can take to improve their posture.

MARK COLEGATE: And how do you make sure, if one of the weak points is people, which it always sounds like, on the whole, it sounds like it often is with technology, what can you do to make sure everyone's up to speed, should you take the whole company off for a day off every six months?

STEPHEN RIDLEY: Yes, invariably people are the weakest link in this. Whether that is someone making an error in clicking on an email that they shouldn't, whether it's someone misconfiguring a system when it's being installed, that is more often than not the headline cause of claims, to one extent or another. Training is really key as part of that from a user awareness standpoint, making sure that people are aware of phishing emails, which are getting more and more sophisticated, and I think that's where we're probably going to see one of the next bits of innovation to pull it back to that, with the likes of ChatGPT and other equivalents coming to the fore, those phishing emails are going to get trickier and trickier to spot. So making sure that people are really aware of not just avoiding the things that would be evident to most people, such as promises of millions from relatives that you haven't seen in, or have never come across, but those that are far more sophisticated than that and much more targeted. And then it's around the governance processes that a business puts in place as well around those, particularly for larger organisations around, how do they go around assessing and assuring their systems, not just at the point of them being installed but on an ongoing basis as well.

MARK COLEGATE: I want to come on to AI and ChatGPT in a second, but before I do, Tom, you were talking about people working from home, and one thing I've seen as a result of that is the idea of what's your work computer and what's the home one has got blended over time. I'm sure we've all, the number of times we've all had someone say oh I can join you on that call but my work computer won't let us do Google Chat so I'll use my home one, or whatever it happens to be. How much of a danger is there of that blending of work hardware and software and home hardware and software?

TOM DRAPER: I think it's a really good example of why there's not a technological solution to cyber as a risk and actually why insurance policies are needed. Because actually your workforce will be, to an extent, actively working around some of the controls we've put in place. Stephen mentioned phishing emails increasing: 76% of our incidents last year came out of phishing emails. So despite team members being educated, being highlighted this issue, and it inevitably will be. Like I said I think phishing emails are going to be the starting point to that where you can get them to run the script and produce something that is very compelling and much more likely to be clicked upon. But I think we'll then start to see it being used in other ways as well, and they'll find other use cases for deploying that, which can just make the whole process much slicker, quicker, easier, cheaper for them to run, which then will widen their potential attack victims as well.

MARK COLEGATE: And, Tom, presumably you can, I'm sure you can do it manually, but you can scrape quite a lot of data off the internet about people and create a very convincing digital avatar of somebody, you know, that when it's presented to you, you think yeah that completely stacks up, I'd go with that.

TOM DRAPER: Yes, exactly, I think that's it. It's weaponising and scaling up are already a concern with social engineered attacks. It's making it more applicable. What I would say, however, there's also a benefit to usingof large language models and AI. We announced in April of this year that our platform is using a large language model to help companies understand their cyber exposure and understand their security risk. So when a CSO logs in and sees there's a vulnerability, they're able to talk to a bot that explains it in more simple language actually what they're being impacted by. So it does scale the attackers, it causes concerns there, but it does enable actually insurers to actually talk to companies in a far more logical way than perhaps we would.

MARK COLEGATE: And whether it's boots on the ground or language learning programmes, you're obviously both, or your organisations are both scanning for what these threats are all the time, so what happens if you spot one in, I don't know, a small company in Westmorland, do you tell all your policyholders in Cornwall at the same time, how much are you running a service that's not just the insurance, it's also a lookout warning system.

TOM DRAPER: I think our record at the moment is five hours between when we've spotted a compromise available on the wild internet and then notified the policyholders impacted by that vulnerability. So if for example you had your SME in Cornwall that had a problem, exhibited an attack, was attacked in a certain way, our R&D team would understand it, look at it and then notify the policyholders who exhibited the same behaviour. And I think from our perspective that's key. Just because everyone's running a Windows machine doesn't mean they're all exposedto the same risk. Just because everyone's in Amazon Web Servicesdoesn't mean they're all exposed to the same risk as well.

MARK COLEGATE: Yes, Stephen, what sort of resource have you got in that space to?

TOM DRAPER: Yes, fairly similar, I would say, but perhaps focusing more at the end where it's more likely to lead to a catastrophic loss across multiple customers. So one of my big things that I don't want to run the risk of being the boy that cries wolf with anything that we do and wanting to have some kind of element of materiality or potential materiality to what we do when alerting our customers, but we're definitely keeping tabs on the risks that could have that big potentially aggregating exposure, such as the Microsoft Exchange vulnerabilities that happened a couple of years ago, SolarWinds, Log4j, those types of incidents, making sure that we can spot those as quickly as possible and proactively contact the customers that are impacted by them.

MARK COLEGATE: And looking at the world of threats, Tom, Coalition, I think you said started in the States, but how geographically specific are threats, do you see a world where you think well if it's in Alabama now, it'll be in Scotland in three months - I'm just thinking about how you keep an eye on where threats develop and how quickly.

TOM DRAPER: Very much so. I would say the bulk of the English speaking Western world are probably under a similar threat environment, because if you're a cyber-criminal looking to attack as many entities as you want, you get to speak English, you write the email once, it goes out to all the teams. They're also generally reliant on similar infrastructure, very similar maturity levels. So it's a very straightforward proposition from their perspective. But we definitely do see, you know, our claims team operate 24/7, follow the sun, we'll have a claim notified in the UK, we'll start to then see claims being notified out of the East Coast, and as teams wake up and that vulnerability has been exploited, it'll start to happen around the world.

MARK COLEGATE: But is there anything, I'll say it in very round terms, the British are more likely, a hook the British are more, likely to attach themselves to but the Canadians don't, there must be some.

TOM DRAPER: So there definitely are, but I think it comes from maturity levels. So for example you will have seen a big increase in Australian attacks recently in the news, probably the last, definitely in April, and that was being driven by a real focus by a number of specific threat actors on Australia as a market where there was opportunity.

STEPHEN RIDLEY: I think there are some geopolitical things that come into play with it, but also there are technological things as well. So I mentioned the Microsoft Exchange vulnerability from a couple of years ago just a moment ago. And we actually found companies in Germany to be far more affected by that than elsewhere, because in Germany they were still running on premise email servers far more frequently than their counterparts in other territories were, who had migrated to the cloud in much greater extent, so those are other mtypes of issue that come to play with this.

MARK COLEGATE: We've got a few minutes left and we've talked a lot around the general environment for cyber at the moment around SMEs and some of the preventative things you can do, on the basis prevention is better than cure, but if something were to go wrong, what are some of the post-event support that you can provide, what are some of the main things and, I suppose, given SMEs are such a broad range of businesses, do you find with different SMEs it's a very different service you'd have to offer one from the other, or there are some elements that are all pretty much everybody'sgot in common?

STEPHEN RIDLEY: So there's a certain element of consistency across it all, but every single attack is very different, both in terms of how it was actually manifested, but also the impact on the end customer. So everyone does need a slight tweak to that main model. But generally the main things that we're talking about are the things with incident response, IT forensics, legal partner support, PR support to deal with both the internal and external communications around it, and then various other service providers that might need to be plugged in after that, but one of the ones that often gets overlooked is the emotional support element to it as well, particularly for SMEs. It can quite often be a very traumatising time for them. So everything is set up to make sure that there is an eye on that aspect to it as well and that things are treated sensitively in that respect as well.

MARK COLEGATE: Tom, what's your thoughts on that?

TOM DRAPER: I think that is the key reason you buy the policy, especially for SMEs, is they don't have the resource, they don't have the number to dial, so anything we can do to solve the claim, not just handle it. We handle a lot of it in-house with our teams. It speeds up our feedback loop so we can see what went wrong, what we should improve. But also, to the point Stephen made, this is the worst time for this client, especially for an SME, it's their personal business, it's their personal assets. We need to solve this; we need to get the money back if it's been stolen; we need to get them back up and running. That's an area that we've had a lot of success in has been, especially the return of funds, so clawback proposition, a lot of theft of crime losses, for example. So yesterday we had $4.8m returned to a small business that they'd lost through a business email compromise, transferred the wrong amount of money, and our team was able to get that back from the banking system. So that's real value-added and money back to their bottom line.

STEPHEN RIDLEY: And cyber is one of those areas as well where, to draw the parallels back to the physical world again, if someone turns up to their building and it's on fire, you know to call the fire brigade. Without a cyber insurance policy, I imagine people rock up and find that similar type of damage to their IT environment, just not really knowing who to call and then that can lead to a lot more of a frantic response as well. We actually had a customer a couple of weeks ago that had this type of incident. They hadn't bought a policy, were in the process of getting a quote at the time but hadn't actually bought it. They were quite a key partner for us on some of the other lines of business. So we were able to still support them through the process and give them some guidance around how it works, but their comment was that they would have just been completely lost if they were trying to navigate their way through that without people who had that wherewithal and knowledge of how to handle these incidents.

MARK COLEGATE: So Stephen to what extent is the amount of business you can underwrite not down to underwriting limits and how much risk you want but how much resource you've got to help people in these circumstances, to what extent might you say yeah we can from an underwriting perspective write hundreds and hundreds of millions of pounds of this stuff, but I've only got 50 people who know what they're doing
and until I've got 60 I'm not comfortable writing more policy, so what do you think of the volume of this?

STEPHEN RIDLEY: Yes, resource isn't an issue for us at the moment, and I don't think it will be in the short term and nor for the industry at large, both in terms of the underwriting stuff but more importantly the fulfilment of the claims. Where the challenge might come is if there is a big bang incident where you've got thousands of companies potentially affected at once, and that's not an Aviva issue, that is a market issuewhere there are relatively small number of service providers that operate in that kind of space. And if it is into the several thousands of companies, that's going to be really tested for everyone I think.

MARK COLEGATE: Tom, what are your thoughts on that and is there a danger that providers think, do you know, this AI is quite good, I can cut corners and where I used to employ people, I've got a computer programme that will cover 90% of it?

TOM DRAPER: I think scalability is a concern for sure. But again that then comes down to how can you service a wider spectrum, what can you do upfront, so the vulnerability assessments that we do, how can you stop the claims happening in the first place; but then I think it also comes down to recruitment and that's something that as an industry we're all very much focused on, how we can recruit the best talent, cyber secure experienced talent. It's an area that we've got great bench strength. Most of our risk engineers, the teams,,they come from a security background, they're not actually insurance professionals. About 50% of our colleagues are from a tech world. So there's definitely a large expansion there that the market can take advantage of.

MARK COLEGATE: Well, on that, Tom, how can you make sure that you aren't recruiting somebody who's really good at this stuff, but one reason they're really good is they've been on the other side of this fence, and what do you do to keep tabs on people after they've left to make sure you haven't been a perfect training ground for them to go off and then do something absolutely horrible that then falls back on an SME somewhere else?

TOM DRAPER: That's a really good question. I think from our perspective most of the areas we're recruiting from are generally the intelligence agencies, so that's GCHQ or the NSA. I think there's a certain level of due diligence that we'd expect of them. When it actually comes to when they move on from us, I think we've got quite a good retention rate of our staff,but also it does become a discussion. Actually one of the biggest concerns anyone should have, the threats that brokers have, considering they hold policy information on all their clients. It's a risk to brokers, that's why they're a potential target. It's a threat to insurers. That's why we need to make sure that our security is top-notch to make sure that we're demonstrating to clients we're doing everything we can to protect them.

MARK COLEGATE: Well, on that point, Stephen, what percentage of brokers do you deal with who don't have cyber insurance, just as a rule of thumb?

STEPHEN RIDLEY: Again, good question. I couldn't tell you I guess off the top of my head, but I would say there's still a fair proportion that don't carry cover themselves. We do provide cover to a decent number of brokers ourselves, but I wouldn't have any idea as to the number.

MARK COLEGATE: No, I was just assuming that you probably wouldn't go out and sell cyber insurance unless you had some yourself, unless you think it's worthwhile for you, you're probably less likely to try and pass it on to your clients.

STEPHEN RIDLEY: Potentially, yes.

MARK COLEGATE: We're almost out of time, but one thing I did want to mention, GDPR. We're coming up fifth anniversary of GDPR. And I know when we've done cyber masterclasses in the past, that's been quite a big topic. So, as a final thought, just get a sense from each of you, what the main consequences of GDPR have been when it comes to cyberspace and innovation. Stephen, can I start with you and then let's bring Tom in?

STEPHEN RIDLEY: So it's a bit of a slow burn I think and certainly far slower than people thought it was going to be. In that two-year implementation period in the run-up to it going live, there was all this chat about all of a sudden you were going to see these whopping great fines being handed out left, right and centre, but the reality is that there's still been very, very few fines actually issued out under GDPR. There's been far more under PECR, the communications regulation around sending spam texts and the like and things like that, but actually far fewer coming about because of data breaches or companies being hacked. What it has changed for the insurance industry is the impact on claim cost, and that's what we saw or, in part, led into the hard market conditions that we've seen over the last couple of years. As we've seen data breaches occurring, even things just like ransomware data being encrypted, technically under GDPR that constitutes a data breach that needs to be reported to the ICO, which in turn requires much more in the way of investigation costs, preparation costs to lead to that. And on the back of those notifications to the ICO, we've then seen much more in the way of litigation being attempted against companies that have had issues. Not a huge amount of it has been successful litigation, but still the process of defending that or at times making small settlements to people led to this inflation of cost, which would historically, and historically in the five-year horizon term, just been a fix the system, pay a business interruption loss and that's it. Having this liability element to the claim is something new that did add an exponential element onto the cost.

MARK COLEGATE: Tom, would you go along with that?

TOM DRAPER: Very much so and especially the litigation side. The liability aspect is probably the biggest game-changer out of GDPR. Effectively, we gave a huge number of law firms, who were previously chasing personal injury or PPI loans, the ability to expand that to include data breach. So we saw immediately after British Airways, immediately after EasyJet, if you're on social media you would have seen an advert for, would you like £2,000, were you impacted by the EasyJet breach, were you impacted by the British Airways breach? And those don't get litigated, they get settled pretty early, but it's still a cost that clients are still now having to incur and defend from.

MARK COLEGATE: Well, we are out of time, we pretty much have to leave it there, but I wanted to get a final thought from each of you. There's one key message you'd want to leave when it comes to cyber innovation or underinsurance of the cyber market, what would that be? Tom, let's start with you.

TOM DRAPER: I think the key message and the take-away we've had from BIBA and other events recently has been brokers are really a key part of explaining to clients their cyber risk, their cyber exposure and transferring that risk, and that's what we're seeing going forward.

MARK COLEGATE: Thank you. Stephen?

STEPHEN RIDLEY: We can't underestimate the amount of education that is still needed in this space for everyone, and that's my number one priority for this year at Aviva is how do we really ramp up that education for our customers, our brokers, to help close that protection gap, to nudge up that 10% of companies that are buying cover at the minute, and get that up to,a much more reasonable level.

MARK COLEGATE: We have to leave it there.,Stephen Ridley, Tom Draper, thank you very much.

STEPHEN RIDLEY: Thank you.

**** END OF VIDEO ****