Insure TV: Cyber Masterclass Transcript

MARK COLEGATE: Hello and welcome to this cyber masterclass with Insure TV in association with Aviva. We are focusing today on the micro and SME market in the UK. There are extraordinarily high levels of under insurance when it comes to cyber. But what are the reasons for it and what can be done to address it to really help clients out in this growing area of risk and threat the market. We'll discuss that. I'm joined here in the studio by George Thomas, Cyber Claims Lead at Aviva, Matthew Clark, Cyber Director, Partners& Group and John Clarke, Cyber Technical Underwriting Manager also from Aviva. Those are our panellists. Let's get things straight underway. Well, George, you're spending a lot of time obviously looking at claims. So what are some of the trends that you're seeing there when it comes to particularly to SME's.

GEORGE THOMAS: In the SME space the SME's are not still immune to ransomware attacks. Just like the large multinational corporations but also within the SME space, they are particularly vulnerable to social engineering attacks and also business email compromise and not only that, they are very vulnerable to payment diversion fraud as well and that's the type of thing that we are seeing in the SME space more and more.

MARK COLEGATE: How much is this SMEs claiming on stand alone cyber policies? And how much is it SMEs getting in touch and saying I've kind of got another bit of insurance, but I'm just hoping there's a bit of cyber in there.

GEORGE THOMAS: It's honestly, a little bit of both. We do often see a lot of a lot of payment diversion frauds on our stand alone cyber insurance policies but on other policies as well we do often see notifications where they're asking if there is any cyber here that's available for us.

MARK COLEGATE: Thank you. Matthew, Partners& you're working with a lot of SMEs as clients just tell us a little bit about the mix of business that you've got and what are some of the trends that you're seeing in cyber?

MATTHEW CLARK: Well Partners& is essentially an SME shop. So we serve a range of microbusinesses and small to medium sized companies, up to the majority probably having up to around £25 million in revenue. We do have clients that are much larger than that, but that's the exception rather than the norm. So our world right now is one where we are trying to get SMEs onto a journey of understanding with cyber risk. I think as insurance brokers and insurers, what we are really struggling with is a landscape currently where SMEs to a large extent think that cyber is something that won't happen to them. We have to overcome that challenge and my day job is to help my colleagues do that and start cyber conversations with their clients in a meaningful way at the SME level.

MARK COLEGATE: And, John, can you give us your views on how some of these cyber risks are emerging, particularly from a risk management perspective, and also when it comes to communicating with clients.

JOHN CLARKE: I think a major focus for the SME market has been far too much when we talk about the this cybersecurity framework, which is a good overall framework for cybersecurity management. There's far too much focus on identify and protect the top two layers, and they're a little bit qualitative. SMEs really do require the same level of technical expertise as the large kind of compatriots, as George was mentioning earlier. So there's different ways of cascading that information down, IT providers who themselves can be SMEs sometimes maybe aren't the best place to get that information through.

Insurance brokers and insurers have a plethora of information available, and they're really kind of catching up with the rest of the market.

MARK COLEGATE: Thank you. Matthew, I want to come back to what you said, though, that a lot of SMEs don't think it's their issue. Cyber is something for the large companies. Why is that?

MATTHEW CLARK: I think there are various reasons for that. If we take just recently the most topical media coverage of of cyber events impacted, the MGM resorts business in the United States, which is a $15 billion business. Many micro and SME companies that see that kind of cyber reporting think well, that's way out of outside anything I can relate to. It's not relevant to me. They also tend to believe themselves to be immune, perhaps because they're using external service providers for their IT that it's something that they outsource or they feel that they don't hold huge volumes of data, so therefore, they're not going to be a target or they're just a small business, and they shouldn't be occupying the attention of cyber criminals. Of course, unfortunately, we know, from all the research and various case studies and survey reports that are available in the marketplace, that the opposite is true. That SMEs are actually attacked far more frequently, and aggressively than larger businesses.

MARK COLEGATE: And John is that because SMEs are less prepared because presumably if you want to perpetrate cyber fraud you've got a trade off? If you hit the jackpot, a really large company, it's a huge payout, but they'll be very well protected versus take lots of little bets, but they're probably quite easy, individual bets to crack.

JOHN CLARKE: Well, I suppose you can argue larger corporations have a wider what we call attack surface. So there's more entry methods in. SMEs in this country employ 50% of the populace. So you've got quite a broad attack surface there to propagate attacks such as social engineering, phishing scams that George was speaking about earlier. So for for one thing, training of those staff members is absolutely pivotal. And it's probably the biggest bang for your buck thing that you can do.

MARK COLEGATE OK. And also Matthew, I'm going to bring George in a second. Before I do. Could you put some numbers on? I mean, we've talked in general terms that this is an area of the market that's underinsured. Have you got any numbers you can put on as to what that level is and what the downside is if you get this wrong.

MATTHEW CLARK: Yes, certainly. Well, I mean, in terms of the general sort of threat landscape that we're all facing right now, the UK government actually puts out its own cyber breaches survey report every year, and the 2023 report, one of the key stats there showed that 32% of UK businesses reported at least one cyber attack in the last 12 months, which is a huge, volume of cyber activity. Imagine if I'd said that 32% almost a third of UK businesses had suffered a fire or a flood in the last 12 months. We'd all be running around with our hair on fire wondering where our fire insurance policy was.

But cyber insurance is massively undersold. There's the different estimates that I've read, range between 15 to 10 to as low as 10% as SME take up of cyber insurance. So all of our work is ahead of us in terms of educating clients in the SME sector as to the level of threat against them, the severity of threat and the frequency of attacks and getting them onto a journey towards cybersecurity, better cybersecurity and cyber insurance as the ultimate blanket of protection.

MARK COLEGATE: George, from a claims perspective, have you got enough resources to deal with the amount of claims that are coming? You know, if this is a growing area of the market and there's a lot of

under insurance, and hopefully over time that changes, do you look around the office and think have we got enough people here to deal with all of this?

GEORGE THOMAS: We do have cyber surge planning in preparation for those type of events. We are quite prepared for the event of a huge amount of business email compromise attacks or ransomware attacks. But also, we are still always trying to increase the headcount for those people who can deal with cyber claims and assess and manage them efficiently.

MARK COLEGATE: And George, you mentioned earlier there's certainly some trends from cyber criminals on how they're targeting smaller companies. Could you give us an example or two of what's going on and why it's such a problem?

GEORGE THOMAS: I think it's social engineering scams again. Social engineering scams are where an attacker impersonates somebody in senior management within an organisation. And they're able to perpetrate fraud, and they can do this by telephone. They can do it via a business email compromise. And then they're able to, divert payments that are meant to go to contractors. And so even for small businesses, not just large businesses. They make payments every day to suppliers and contractors. Even for conveyancing solicitors as well, we see that quite a lot. They're able to divert the payments that were meant to go to to those people and they'll go to the attackers. Once they're in the attackers bank accounts, they will then divert the payments around to the separate bank accounts and then we're unable to recover the funds, as are the bank and the police.

MARK COLEGATE: So I get it, if somebody was able, you are my boss, and I got an email that seemed to come from you, but you mentioned phone as well. I mean is this where AI is taking us now?

GEORGE THOMAS: Well, we mentioned AI. I think there are a couple of rumours around the market that there are attackers that are able to use voice changers to impersonate senior management and able to perpetrate fraud. We haven't seen that yet within Aviva but I think that's certainly something on the horizon. And what we're seeing with the telephone is that we are seeing attackers being able to use the phone to be able to ring those within the office. So perhaps an executive assistant or somebody who's not a senior manager and able to gain access to the insured's bank account or an organisation's bank account and be able to divert payments in that way.

MARK COLEGATE: John, how do as Aviva help provide education on this? Because I suppose listening to that the short answer is, don't trust anybody unless you're sat down face to face with them if they're discussing internal movement of funds and a business.

JOHN CLARKE: IT is broad. You can have somebody who's a developer. You can have somebody who's a network engineer, security architect. It's very, very difficult to sort of pin down a particular person in that SME who might have to focus on cybersecurity. But there are ways of educating and getting yourself up to speed on the various risks that you know are prevalent to SMEs. I mentioned previously that a lot of SMEs outsource their IT, and I think Matthew spoke about it as well. In a recent science direct study, 93% of those particular organisations are themselves SMEs, so they might have sort of a small area of expertise in cybersecurity. So trying to cascade the information down through insurance brokers and in the insurance marketplace is probably a more advantageous way and that study kind of backed that up as well. So there is material available. The National Cyber Security Centre is a really, really useful place to start effectively for any small business or any organisation.

MARK COLEGATE: Matthew just of interest. If you are a small business that has outsourced a lot of what you do to an IT third party, why is that a problem? I mean, they're the experts, not you.

MATTHEW CLARK: Well, it's often super convenient for businesses of all sizes, actually to use external service providers. It generates efficiencies, it enables them to use expert platforms and systems to enable them to perform their day to day tasks. That's fantastic. But with every use of technology comes new risk. and if you're outsourcing services to a third party you're essentially extending your supply chain vulnerabilities to encompass what that third party is doing for you. So you have to make sure that your own view of your cyber risk encompasses your reliance upon those third party providers as well. You need to understand what they're doing with your data and how they're securing the systems and data that you're relying upon that from them. The other important thing to to bear in mind is that in the UK, the data protection legislation makes it very clear that even though you might be using third parties to manage your data, for example, you still have the liability for any breach with that data, so you have a direct responsibility to the data subject, so using those third party systems creates efficiencies, but it doesn't absolve you from any blame if things go wrong.

MARK COLEGATE: So you can't fundamentally as a business, you cannot outsource your responsibilities.

MATTHEW CLARK: You can't contract out of responsibilities. That's right.

MARK COLEGATE: Thank you. John, I want to come back to a theme from a little earlier, which is this idea that not all but some SMEs will say, well, this is a big company problem. Is there some truth in that in a sense as to why they don't interact with cyber policies on the basis that actually, for you as providers, you've created policies that have got all the bells and whistles on because the first people who you've gone to are the big companies, and actually you're offering something that's got expensive bells and whistles that really they don't need and therefore they just say thanks, but no.

JOHN CLARKE: I think the the big companies in the press have had kind of more coverage about the losses that they've faced and the loss that they suffered the attacks that they are actually able to recover from. It's the small companies that have gone bump or the small companies that have some kind of ransomware attack or some kind of, you know, damaging attacks their infrastructure that you don't hear about in the press, and they are equally as devastating, you know, proportionally to their size. SMEs - the major way in, as we've touched on, is that social engineering piece. But all it takes is what we call open source intelligence, which is just looking at any kind of publicly facing infrastructure.

So we talk about the Internet, we talk about kind of marketing that you put out. That's what hackers are using to try and forge attacks. They're going on LinkedIn. They're trying to find out who the Finance Director is. They're going on to your website. They can get email addresses, telephone numbers. So SMEs might be actually putting out quite a lot of information about themselves that they're not too sure about, or they're not sure that it can be used against them and they're equally as kind of should we say, juicy for the cyber activists.

MARK COLEGATE: And Matthew, presumably a lot of people as employees will also have their own digital presence in their capacity, as individuals. What are some good policies to have as a small business, that sort of make sure that those two worlds are kept separate?

MATTHEW CLARK: Yes, this is a very crucial question. And one of the starting points for us in discussing cyber risk with SMEs is that they should have good corporate governance in place. And that means having the appropriate processes and procedures that they communicate effectively to their

staff. To make sure that staff are behaving within the confines of what their company feels are sensible rules. So that could be things like use of social media, particularly when it comes to using company devices to access those systems and it could be the use of third party software systems using company devices as well, other kinds of networks and systems. So there has to be some governance to tighten up controls there. As, of course, it extends the company's general attack surface.

MARK COLEGATE: But I'm wondering as well down to specific things like I don't know, I put on Facebook 'We're off for a wonderful week's holiday with the family' or whatever and then somebody sees that and phones George and says, I've been talking with Mark, I know he's away this week. I wonder if you could just do the following and send it through. I mean, can you have policies that even cover the amount of information you put out about yourself? Or is that getting a bit constrictive on employees in their capacity as individuals?

MATTHEW CLARK: I think it's important as part of those processes and procedures to have effective internal financial controls. So, for example, in terms of what we were just discussing around social engineering attempts and phishing attempts, it's useful for a company to have very strict rules around who can move money, who can respond to requests to move money or requests from counter parties to change bank account details, things of that nature and those have to be strictly adhered to. Otherwise, you could be exposing yourself to unwanted attention from cyber criminals intent on performing those funds transfer frauds.

MARK COLEGATE: And recently there was a Dear CEO letter that went out talking about the importance of making sure there's value for money and I think sort of cyber was part of that. Can I get your thoughts on that first? What are the the key elements in that? And how does that make or how should that be, making insurers and brokers think about what they offer?

GEORGE CLARKE: Yeah, I think it's important to kind of look at the whole package in terms of what the cyber insurance policy provides. It's not just money that cyber insurance policies provide. It's also the response element as well. And so when you look at what cyber insurance policy provides, you've got the first party elements. The first party elements are the business interruption funds that they provide and the indemnities they provide but then also you've got to look at the response as well and the response part is especially crucial for SMEs. And that's the ability to be able to instruct IT forensics teams and also to be able to instruct lawyers as well to be able to provide that critical response in terms of advising insureds and organisations as to what their contractual and regulatory obligations are as well.

MARK COLEGATE: So when you've dealt with a claim and you're dealing with the customer in the round with cyber do they say, 'Thank goodness there was a pot of money at the end.' or is it 'Thank goodness you got the right people in touch at the right times that helped unpick this mess.'? What afterwards is the thing, the feedback you get that provided the best value?

GEORGE THOMAS: Maybe I'm being a little bit biased, but I think they always thank us for the help that we provided rather than the money but I think they're also thankful, thankful for the money as well, again it's a little bit of both. So when you look at a ransomware attack, for example, you've got the response elements, so you've got the cybersecurity response and you've got the lawyers, and then you've got the PR and potentially credit monitoring as well and all those form into kind of a crisis management team. And that really is the backbone of the team that would help an SME once they're going through an attack, and but then also on the latter end of the claim, you've then also got the business interruption and then potentially the third party liability stuff as well that you're still helping out with. So you're getting that help along the way. But then you're also getting the funds at the end if there is a business interruption

loss or or there is a litany of third party claims, and then also, just remind everybody that appointing these experts aren't cheap as well. And so if an insured had to appoint them by themselves, that would cost a hell of a lot of money.

MARK COLEGATE: Well, as I asked you that question, I could see Matthew - so let's bring you in.

MATTHEW CLARK: I mean, you're absolutely right. The real benefit that we see our clients gaining from having an insurance policy is the breach response service. The first response that a client has, when they suffer this kind of attack, regardless of what type of cyber attack it is, is blind panic often times. They just don't know who to speak to. They don't know how to get the advice that helps them to respond to and recover from the attack. So having access to a kind of break glass push panic button 24 7 response helpline is massively important. It helps them feel as though they're not going through this alone that they have somebody who's on hand to triage the problem for them and then deliver using insurers, panel providers, whatever service it is that helps them to recover from that attack. And frequently that is either a combination initially of legal advice around potential notification to the Information Commissioner and IT forensics to understand how the bad guys got into your system in the first place. And those are often very critical because SMEs lack the ability to access those sorts of services and knowledge themselves.

MARK COLEGATE: John, how do you make sure you've got enough of that third party expertise capacity on hand? Because again, if this is a growing market, if you're working with, I don't know, eight law firms now, presumably you can do the math and think, oh, we better be working with 16 by this time in 2025 or 32 by 2035. I mean, how do you make sure you've got enough people online to help and that they themselves have got enough capacity?

JOHN CLARKE: George mentioned the kind of expense involved with appointing third party experts. If you do suffer an attack and you go with a big name in the response or the instant response category, they're going to be charging upwards of £1500 a day. £2k maybe £2.5k per day. You mentioned the letter that was sent to CEOs or the Dear CEO letter from the FCA in regards to value for money. To directly address that, Aviva have worked with the product team to strip out parts of the of cyber insurance coverage that aren't massively important. They are very important, but they're not the priority for an SME. That as you mentioned before Matthew, the blind panic that they suffer from when there is an attack. So the respond product from Aviva, which is available to sub £1 million turnover companies, provides nil excess or very little excess, provides you with a phone number to respond if there is an incident. So you switch on your laptop on a Friday afternoon because you've been at the pub. That's why it's Friday afternoon and you switched it on and all of a sudden you're met with a ransomware attack. You can pick up the phone, call the hotline that's provided and get instant access to a response specialist.

MARK COLEGATE: Ok, thank you. Thank you for that. We've talked a little bit about how this is growing out of the market. Matthew, how sensitive are clients to price on this because we've heard a lot, you know, it's a fairly common thing. People say it's a cost of living crisis. Business is under pressure that a lot of people are just put off getting cyber.

MATTHEW CLARKE: There's no doubt that cost is an issue and the perception, certainly three or four years ago pre-pandemic was that cyber insurance is something rather exotic and and difficult to obtain and expensive and unaffordable for small businesses. I'd like to obviously mention the insurance market has gone through a rather dynamic period since 2020 - the cost of cyber insurance has increased. The

line sizes that insurers are willing to provide has dropped, insurance underwriters want clients to have more
skin in the game with bigger excesses and retentions. It has been a very tough landscape to operate in as an SME broker. Having said that, I think now the cost of cyber insurance is more in tune with the risk that SMEs are running without necessarily realising it. It's incumbent upon brokers like me to be able to position contextually the conversation with clients as to why the price is what it is. And it's very easy to show that using the various statistics and case studies and information available in the marketplace, that cyber is very often now the number one risk that our clients have in the SME space without them necessarily realising it. So there's a certain element of reassuringly expensive pricing around cyber insurance. It needs to be considered alongside lines like professional indemnity and product liability for SME businesses.

MARK COLEGATE: How do you take a client along that journey, where they get to a stage that say 'Yes, it's reassuringly expensive' rather than 'Oh God, the only thing that I haven't got insurance against is somebody telling me I have to take out more insurance.' ?

MATTHEW CLARK: I think before clients can understand the value that insurance brings, it's necessary to position the conversation around what cyber risk is to make sure they have an understanding of that and what it can do to their business. Only then can we really relay and intrinsically demonstrate the value of insurance and the breach response service that comes with it. So for us the discovery process with clients comes first, assessing their preparedness for risk and getting them in a better position in terms of their cybersecurity then comes second. And then, lastly, that makes the insurance journey a lot easier.

MARK COLEGATE: And if you're a broker listening to this thing, that all sounds great in theory. But how long do these journeys take? If I'm going out and talking to a small client who doesn't produce a lot of premium, I've got to provide them a good service, but it must be tougher to get out of bed and think, oh, I'm gonna have six months of conversation before you know there's some business at the end of it.

MATTHEW CLARK: There's no doubt this is a marathon rather than a sprint. But the opportunity is huge I think by some estimates, the current value of the cyber insurance market is around $14 billion globally. It's estimated, though, to be closer to $85 billion dollars by 2030. So although it requires a lot of upfront investment right now, the opportunity is huge for brokers and insurers to to tackle this thorny issue in the SME space. (This section of the video experienced a technical difficulty– some content is repeated).

MARK COLEGATE: And George, you were unpacking some of the examples of what you're seeing in claims at the moment, particularly around payment diversions. But could you talk through in a bit more detail some of the other trends that you're seeing?

GEORGE THOMAS: Yeah, it's not just ransomware or social engineering. I think one of the other big claims that we see is business email compromise. And we see a high frequency of business email compromise cases. That is not just for the purposes of committing payment diversion fraud. This can also be to commit data exfiltration, which is taking personal data, stealing it and selling it on the dark web, or also, in order to further complete phishing campaigns to other organisations as well. And business email compromises can be quite expensive because again, you've still got to do the response piece. You've got to do the IT forensics piece as we touched on earlier and then you've also got the legal and contractual obligations. Often times you'll have contractual obligations to some of your customers that you may not realise that are written into the contract if you've had a cyber incident, and then you've also got the obligations to notify the ICO and to notify any data subjects that have been impacted. And so it can become quite costly, even if there's no payment diversion fraud at the end of it.

MARK COLEGATE: And this is probably a very unfair question to to ask you, because I appreciate there's a real plethora of cases that you'll be dealing with, each of them is unique. But when someone has been cyber compromised, how long can the business keep running before they realise it? Is it pretty much instantaneous or are there quite a lot of plans? It happened eight months ago we had, you know, this has been chuntering on for ages.

GEORGE THOMAS: Yeah, you'd be surprised at how long a threat actor can sit within an organisation system before they pull the trigger, so to speak. I've seen threat actors sit within systems up to to 9 to 10 months, but most organisations do notice quite quickly. But even if they notice after seven days or even two weeks, the clock is still ticking. Once you do realise in terms of your personal data obligations and then also trying to identify, contain and mitigate the breach to achieve a reasonable outcome.

MARK COLEGATE: So presumably, this won't solve every problem. But a certain amount of being wise and self help is a good idea. So what are some of the things that companies can do themselves to sort of mitigate risk, to go back over things? Double check? Just so that, you know, even if there is a threat actor in there, they find them sooner rather than later.

JOHN CLARKE: Yeah, I think the first and kind of most important thing I mentioned earlier is training. So training for all staff members who have access to any kind of Internet facing device. Training on the threats of potentially what might happen if they're going to click on a link that might be diverting them to somewhere else, the dangers of not enabling multi factor authentication on their phone because they can't really be bothered. Just going through some of the kind of basic cyber hygiene is the biggest bang for your buck thing that you can do. It's a lot of the times it's free if you want to go and use for example, the National Cyber Security Centre have a training module if you want to use third party implementations as well. It's not massively expensive, so training is kind of first and foremost.

Secondly, there are technical implementations that you can work through. I'm not going to go into great depth now but things like enabling multi factor authentication, things like actually just having a password that's longer than 12 characters. If it's three random words, that was the guidance a few years ago, so three random things around you can exponentially multiply the time it takes for somebody to brute force that password. And if you take an SME that they're less likely to have kind of purpose built systems internally, they're gonna be using a lot of software as a service applications and platforms, which will then mean there's lots and lots of passwords that they're going to potentially be using. So implementing a password manager to make sure that you're using a different and distinct password in every single different application that you're using, it makes it incredibly difficult. A kind of layer above that is, as I said, multi factor authentication on all those different systems. So there are, you know, multiplex of things that you can do and they're not massively expensive either, that it's just about being in the know. It's about talking to your broker, your insurer, just to figure out what kind of things should I be focusing on? We have a statement of fact at Aviva, which is nine things. If you go through and work through those nine things as an SME you're probably…I don't want to check a stat out there I might get wrong, but you're above the kind of national average for how secure you'll be.

MARK COLEGATE: And George, in your experience, when you look at cyber, how much of this has been human error and how much has this has been, I think what John referred to as brute force, you know, it's computing power, plus time? You haven't got a chance.

GEORGE THOMAS: Yeah, often times it can be difficult, once an attack happens to be able to really drill down to the root cause but when we do, I would say it's around 70 to 80% result is because of human error and then 20% is via brute force or open source and open source reasons.

MARK COLEGATE: Thank you. Matthew, can I get your thoughts on what you can do to self help and not least because Partners& is an SME in its own right. So what are the challenges you've been mentioning? Things other people should do? What have you been doing as an SME?

MATTHEW CLARK: Well, that's a great question. We have ourselves chosen to go down the Cyber Essentials route. I'm a big fan of Cyber Essentials. Cyber Essentials is something that was developed by the UK government. It's essentially a cybersecurity certification programme for businesses. It takes them through five basic steps towards good cybersecurity, many of which we've just been discussing. But it's things like how to craft a robust core IT system. How to manage access to your to your system using authentication layers, uh, how to guard against malware attacks, how to train staff. It's a little bit of self help, really, for SMEs, it's a very convenient way of self certifying actually, there are two levels to it. There's Cyber Essentials and Cyber Essentials Plus. The difference with Cyber Essentials Plus, which is what my firm has now has is that you have to be externally audited and assessed and certified as part of that. But it's a relatively straightforward, easy process. It's low cost. It protects you against something like 80% of common cyber attacks. So it's a very effective way for most SMEs to mitigate cyber risk in their domains.

MARK COLEGATE: John, in your experience presumably SMEs when they get interest in the idea of cyber and say, this is an issue we need to take seriously that there's got to be an internal champion. Somebody must pick up that baton at the start. In your experience, are there particular types of people or particular roles they have in an organisation?

JOHN CLARKE: Well, in a previous role I was risk management focused and I had an organisation on a Teams call, and I was going through a bit of an open source intelligence gathering exercise with them and whilst I was on the call with them, I was able to find their open, remote desktop server and that was a wake up call for the business owners who were on the call. But more often than not, it is outsourced IT. It is internal IT kind of experts, or managers who are pushing to get that cover. But it also comes from brokers like Partners& in terms of the expertise that they bring to the table and the conversations they open up with those clients, which ultimately leads to the idea of maybe I should explore it. And then maybe I should, further investigate it.

MARK COLEGATE: Matthew, let me get your thoughts on that with just with with your client base. Who are the people who respond most quickly with an organisation when you get that cyber conversation going?

MATTHEW CLARK: Yeah, very often it's the IT manager or IT director that we speak to, smaller businesses may not have one. So it could be that they outsource that function to a service provider. We will happily speak to their external IT service provider. If it's a micro business, you often find that you're talking to the entrepreneur, the founder behind the business and they're wearing lots of different hats. So it's quite a broad church, but ultimately it generally boils down to whoever's responsible for the IT for the business.

MARK COLGATE: And George, I suppose the world divides into two cultures. There's those who get technology and digital stuff and can speak that language, and then the bulk of people that can't and don't, so how do you knit those two communities together? When you come to the claims process where

everybody in an organisation has to understand why you've come to the decisions you have when you get some resolution around an incident.

GEORGE THOMAS: Yeah, that can be difficult at times. I think one of the benefits of having cyber insurance is that you've got those incumbent panel vendors. So you've got the digital forensics and cyber security response consultants, and you've also got lawyers who specialise in data protection law and they're able to simplify the jargon into plain English.

MARK COLEGATE: Well, we are almost out of time, So I want to finish by getting a final thought from each of you. There's one thing that brokers or SMEs can be doing to think about getting better and more effective cyber coverage. What could that be? John.

JOHN CLARKE: I think knowing what's available across the market, Aviva in this space are working, you know, very tirelessly to try and provide suitable products for the SME market in respond it, you know, chops out a lot excessive premiums that might exist for some £1 million turnover organisations. So knowing that is available is kind of step one. Step two is making sure that you're keeping up to date with everything you possibly can in that space. And it can be difficult, but you know what Matthew's speaking about in terms of Cyber Essentials, which comes from effectively GCHQ, keeping up to date with the National Cyber Security Centre, they're two of the best things that you can follow and and get your information from.

MARK COLEGATE: Thank you. Matthew.

MATTHEW CLARKE: I think, given the size of the opportunity available to us, brokers and insurers just have to work together to try to make this journey easier for our clients. Insurers have enormous wealth of information and technical capabilities, given their breach response partnerships. If they can make that information and trend analysis and claims data more readily available to retail brokers like myself, it just helps us have those conversations with clients.

MARK COLEGATE: George. A final thought.

GEORGE THOMAS: Yeah, I think it's market collaboration. So insurers, brokers and then the vendors that we use on our claims as well if we all work together and share information we're able to provide more education to SMEs as well and I think that's only going to benefit everybody.

MARK COLEGATE: We have to leave it there. Thank you so much for watching. Do stay with us, though. We've got an interview coming up now specifically on Aviva's Cyber Respond product just remains for me to thank our fantastic panellists today here in the studio.

George Thomas, Matthew Clark and John Clarke from all of us here. Goodbye for now.

END OF TRANSCRIPT