SOFIA GERAGHTY: How can companies improve their security standards to make sure that they secure cyber cover. I'm joined by Alana Muir, regional cyber senior underwriter at Aviva. Hi Alana.

ALANA MUIR: Hi Sophia.

SOFIA GERAGHTY: So my first question for you is do most companies have good cyber mitigation in place?

ALANA MUIR: Sophia, it's very much a mixed bag. Very few firms have the right controls in place. I have started to see a bit of an improvement though over the past nine months as clients have started to understand their cyber risks a bit better. In terms of where I would like to see an improvement, I would like to see all the clients get all the basics right. For me, the number one basic is staff training. So you could have all the technology controls in the world, but as soon as you put a human being in front of a device, all bets are off. You know, they could disable the security. They can invite malware into the organisation and all by accident. So definitely number one would be staff training.

In terms of the technology controls that I would like to see, it would be things like password management, good patching processing. So like a good patching process would include timelines for critical patches and testing. Automate the patching where possible, particularly if they've got a lot of remote workers. Your antivirus and firewalls as well. I mean whilst these are very basic forms of control and they are always out of date, and only respond to known codes, they can be likened to having a roof and windows and a door on your property to protect against weather damage. They won't prevent it completely but they will add a layer of defence.

Other things that I would like to see are system hardening. Clients should really look to actively reduce the attack surface, and by this I mean they should be looking to remove accounts or services that they don't use, put tougher controls on admin access. They should make sure user credentials are withdrawn when someone leaves the organisation, and they shouldn't have any passwords on there that are in the default mode. I would also expect clients to have business continuity or disaster recovery plan. I mean most organisations have had these for years for the likes of fire and floods, but it's only been in the past few years

that they've began to include cyber risk. And they need to test it, because if they don't test it, it's a bit like having a fire alarm and never actually checking to see if it works.

Multifactor authentication, that's very popular, very topical right now. I would expect it where necessary, so by this I mean on remote access or admin passwords, that kind of thing. Segmentation, we've talked in the past about, you know, ransomware and ransomware is rife, there's no getting away from it. And with new zero day attacks, you can't prevent it from happening, but if you segregate or segment your system, you may be able to isolate it to one area and continue to operate. You've got other things like encryption and for me a top-down approach. So by that I mean someone on the board who takes responsibility for cyber risk and putting cyber risk management in place. You can't prevent a cyber risk from happening but a lot of these costly attacks could be avoided by following best practice.

SOFIA GERAGHTY: There's been lots of talk about supply chain as well. How can clients get a hold of their supply chain risk?

ALANA MUIR: The best way to manage supply chain risk is to manage it holistically. Now by this I mean that directors should look to look at what data they hold, where it's held, who has access to it and what controls are around it. They should do the same for their systems as well. And if they have any critical data or critical systems, they should consider putting extra controls around these. If they use outsource service providers, then they need to form part of this process because they act as an extension of the insurance business. Now when I sit in front of a client I say what due diligence have you done with your outsource service providers, and normally they say well I'm not an IT person, I wouldn't know where to start. Well the good news is clients don't have to be IT people, they just ask how do they protect their data. You know, get a handle on how that outsource service provider protects your data. Ask them about their business continuity plan. It's been known in the past that some outsource service providers have failed because they failed to test their business continuity plan. So ask about it.

You could have really strong employment procedures within your organisation. For example all your staff might have to pass disclosure checks, but do the staff at the outsource service provider? So it's just asking these things and making

sure you're not disadvantaged under contracts, and making sure that your contracting with somebody who's got professional indemnity insurance to give you a chance of recourse if things do go wrong. If anybody deals with an outsource service provider, my advice to them is prepare for them to fail. And have a fail over procedure in place. So if they go down, what do you do? Do you have another provider who can pick up the slack; if not, do you have an offline backup or data centre that you can switch to?

SOFIA GERAGHTY: So we speak a lot in cyber about how companies can improve. What are companies already doing well?

ALANA MUIR: The companies that are managing cyber risk well are giving it the same strategic priority as financial and operational risks. So historically cyber risk has been handled lower within organisations, and this is because it hadn't risen to the same strategic level as financial and operational risks. And that's because the financial and operational risks had more rigour, more regulation and more control, and particularly directed experience around these areas. This led to cyber risk being narrowly siloed within IT, which meant it was handled lower in the organisation. Now, if a company organise or works in that way, they could end up in trouble. For example, if you don't have the same focus on cyber risk, you couldn't really make a decision about a sales and marketing campaign for example without considering the cyber risks of the business. And if you did, or you didn't, you could end up in hot water and you could end up facing a GDPR fine on the back of it.

So, in terms of the ones that are managing it really well, they have somebody on the board responsible for enterprise-wide risks, so across the board. They make it a responsibility of everyone within the organisation to take it seriously. And by this I don't mean penalise staff if they make a mistake. They make it easy for staff to come forward and actually say that something's gone wrong, so then they can get a handle on the issues. They look at the risk holistically. I keep using that word holistically because it's not just looking at individual controls, it's looking at how humans interface with their system, and then lastly if they do buy a new tool, a new product to protect their system, really understand what it does and more importantly what it doesn't do for them as an organisation.

SOFIA GERAGHTY: So we have a lot of viewers watching who are brokers, how can brokers help their clients get cyber cover?

ALANA MUIR: I would say the best way to help is to ask all the additional questions in advance and prop forms have come a long way. But if a proposal form is to ask every single question, for every trade, it would be really long. It would be far too long. And unfortunately what happens is if the broker doesn't provide any additional information in advance, there's a lot of toing and froing between the insurer, the broker and the client, and it holds the whole process up for the client to obtain cyber insurance. A good example would be if they look at the manufacturing industry for example. So, historically, manufacturers operational technology wasn't connected to the internet. So it didn't have the same controls as their IT. So there was a bit of a discrepancy between the operational and the information technology.

Now, when we see a manufacturing risk in, a lot of insurers will want to know are the questions in the prop form also relevant to the operational technology? And if it's not, it could be that it's specialist equipment, it needs its own suite of tools, but it could be that actually it doesn't have the same controls. So these are the kind of things that we would need to know. Also if a question is answered negatively, then provide some commentary around this and there could be legitimate reason for it. I've seen in the past, organisations who hold medical data for example and there's no encryption and the risk has been declined by many markets. But actually when you drill down to the nitty gritty of it, you find out that this is because the computer didn't support newer technologies but they took it offline and they enabled multifactor to access it only in person. So they did everything they possibly could but if that information was provided up front, they probably would have got a lot more quotations.

SOFIA GERAGHTY: So it's not necessarily a bad risk. It just wasn't made obvious to the carrier.

ALANA MUIR: Yes.

SOFIA GERAGHTY: And I guess as an insurer, are you being really picky with who you cover now?

ALANA MUIR: So Aviva have got a really wide appetite. We look to partner with firms who have got I would say basic cyber hygiene in place. And by that I would mean, your backups, your password management patching etc. We also like to

make it quite easy for brokers to obtain a quotation with Aviva. We've got for example, if it's an SME firm up to £50m turnover, they can get a quote from Aviva in under two minutes from our fast trade platform or Acturis. If it's larger than that, it would either come into myself or one of our 600 underwriters. We've also invested in artificial intelligence that identifies underinsurance on our existing portfolio. So if we have a client say a property customer who doesn't buy cyber insurance, we will provide a cyber coat 30 days in advance and it's there ready for the broker to pick it up and discuss.

SOFIA GERAGHTY: OK. And just finally, if we're looking at smaller brokers, so in hard market it can be the case that smaller brokers feel like they can't get in front of underwriters, they can't get the cover. Do you have any specific advice for them smaller brokers?

ALANA MUIR: Firstly what I would say is invest in your staff, upskill your staff so they know the right questions to ask the customer, and also how to explain what they need to do to obtain cover. I've spent a lot of time on the broker education piece myself running through all these seminars and trying to build a cyber community where we can all share information in the insurance industry and also with the end customer. Aviva have also invested in a kind of broker training platform, and it's got like nine cyber modules where they can obtain CPD points and covers everything from the likes of wordings to claims. Secondly, for the smaller brokers, I would say pick the right partner really. So work with insurers who have got good wording, have a good reputation and have underwriters who will support you and really understand where you are at in your cyber journey.

SOFIA GERAGHTY: Unfortunately that's all we've got time for. Thank you so much Alana for coming in today.

ALANA MUIR: Thank you.

SOFIA GERAGHTY: And thank you for watching.

END OF INTERVIEW