Watch: Insure TV Masterclass - Cyber Resilience

MARK COLEGATE: Hello and welcome to Insure TV's Masterclass on Cyber Resilience. I'm Mark Colegate. And today we are going to be focusing, in association with Aviva, very much on the SME market, and some of the organisations and resources that are out there that can help you and your SME clients to fight back against cyber risk. Well, to discuss all of these topics, I'm joined here in the studio by three experts. Let's meet them. They are: Stephen Ridley, Head of Cyber at Aviva; Ian Kirby, Chief Executive Officer of the National Cyber Resilience Centre Group; and Ian Hickling, National Coordinator of Police CyberAlarm

Well, I'm going to jump into a little bit more around your background of where you fit in the cyber ecosystem in a minute. But, before I do, I just wanted to start by getting thought from each of you around why this is such an important topic, particularly for SMEs. So have you got an anecdote or perhaps a statistic that can really give us a sense of why this is such an important conversation, Stephen?

STEPHEN RIDLEY: Sure. So I think cyber is now one of the most fundamental risks that businesses of all shapes and sizes see, and we just carried out some research over the last few months that points to the fact that SMEs in particular are now almost five times as likely to suffer a cyber incident as they are a fire in their premises. So there needs to be a mind shift around an insurance procurement process in particular, and we need to start considering cyber as much higher up that risk register for these businesses.

MARK COLEGATE: Thank you. Ian Kirby, what would, if I had to challenge you with one statistic to get us thinking, what would that be?

IAN KIRBY: That's a great question, but would it shock you if you were to hear at the moment the total losses reported, bearing in mind cyber and fraud are hugely underreported but at the moment they total £2.3bn in the last year.

MARK COLEGATE: And that's the reported figure?

IAN KIRBY: That's the reported figure. Obviously, we don't know what we don't know; however, the estimate by the government is that potentially every 20p in the pound is lost currently to ransomware.

MARK COLEGATE: Thank you. Ian Hickling?

IAN HICKLING: I think for me it would be the total number of incidents that occur for any business. A lot of it is happening and people are not aware of it. It's massively underreported. It's probably less than one in five, are the incidents that are reported. And if you look at any sort of statistics around now, you can go and search for them, and those people will say it's anything from £3,000 is what it costs a small business. Some businesses that could be almost fatal for them as a small business, and we need to look at this and how we can improve it so that businesses survive beyond that incident. And

what can we do to save them money, by protecting themselves, but also save them money in the event that they are almost likely to become at some point a victim.

MARK COLEGATE: Thank you. Well, in terms of where you will fit within the cyber world. So, Steve, let's start with you, what's Aviva's particular interest around the SME space when it comes to cyber?

STEPHEN RIDLEY: Our main interest is in ensuring there is strong resilience for UK plc by providing cyber insurance to companies of all shapes and sizes in this space. And we know that cyber is probably where there is the biggest protection gap at the minute in the country, where, you know, an optimistic estimate, it's somewhere between 10 and 15% of companies that are buying cyber insurance at the minute. For SMEs that's likely to be much lower than that. And actually how do we help get the message out there around how businesses need to be protecting themselves in this space, and taking it much more seriously as a risk and ultimately helping to close that protection gap. And that's a big part of the reason why we're looking to work with the National Cyber Resilience Centre Group and Police CyberAlarm to help in amplifying that message and talking in consistent and clear terms to these businesses around kind of why it is so important for them.

MARK COLEGATE: Thank you. Can you tell us a little bit about the National Cyber Resilience Centre Group?

IAN KIRBY: Yeah, sure. So I am, as you've introduced me, I am the Chief Executive of the National Cyber Resilience Centre Group, which is a network of nine regional cyber resilience centres, who are based geographically across England and Wales, and there is also a centre in Scotland. They are the shopfront, if you like, and they form the national group and I provide the support services along with the workplace-ready student talent pipeline, called Cyber PATH, which we may touch on later. The whole point of this is that I am also a serving police officer, senior leader within the police and a rank of detective superintendent. Prior to this role, I was head of cyber for the east of England, coordinating the response across seven forces. I've sat across the boardroom with companies who have suffered fatal cyber incidents. And I've taken that experience onwards to my new role to try and build their cyber resilience, take them on that journey so that when they do suffer a cyberattack, because I don't want to introduce fear, but it is highly probable that we will all experience that some point in this modern day and age are cyber incident, but it's how quickly you bounce back from that. So, essentially, I simplify this in my own world as being crime prevention advice but in the modern day and age; hence why this is a police-led initiative.

MARK COLEGATE: And in terms of the proposition, so if I were a small business and I said OK I'm going to go along to one of these regional centres, let's say in the east of England, where you were prior to this, what's the proposition? Do I have to pay for it, is it about sort of making sure the equivalent of my digital windows and doors are locked, are you providing help after an incident, what do you do?

Watch: Insure TV Masterclass

- Cyber Resilience

IAN KIRBY: So if you were to approach the regional centre within your location following a community event or someone popping in, because we have officers that are walking the high streets, popping into businesses, encouraging you to become a member, which is entirely free. This is Home Office funded, police-led, so therefore again it's that crime prevention initiative. It's entirely free to join your local centre. And when you become a member, you will be given learning material along the way. Because again we recognise that within the SME community and micros, those startup businesses, cyber resilience probably isn't on the highest list of your priorities; expanding your client base, paying your staff, paying the bills, are more likely to be higher up the list.

So we take you on that journey. Because in the beginning you don't know what you don't know, and then that journey is entirely free, as I say. And along that learning journey, you, and once you become more aware of your own risks and for instance you're running a website that maybe has payment portals, take online orders, etc., you then, if you wish, can take opportunity of hiring in some technical services, which are provided by my Cyber PATH talent, workplace-ready talent pipeline. And these are vastly reduced cost to the client, as opposed to perhaps some technical services that are offered by larger organisations. And again we are, because we are police, we are that trusted brand in a very complex, cluttered cyber landscape.

MARK COLEGATE: Thank you. And, Ian, you can tell us a little bit about police CyberAlarm and, again, where would it fit, what's the proposition?

IAN HICKLING: It fits nicely into that, because a lot of people are just not aware of what's happening and how many times they're being attacked and who's trying to get into their network. And the Home Office have funded a project called Police CyberAlarm. And that is distributed freely. It’s a free piece of software, which organisations with any sort of commercial firewall can install. And I suppose if you equate it to the real world, it's a bit like having CCTV, watching the front door of your business. And if somebody was coming along, trying the front door of your business, trying to get in and failing and then keep going door by door by door, you'd want the police to know about it.

So we collect that information about where they're coming from, what they're trying to do. And from that we can build up a picture. And then we can share that with the protect teams in local forces, with the cyber resilience centres, and you can give a better informed advice locally and say this is what we're seeing, these are the types of attack, this is where they're coming from. Other things that we do with it is if people have installed it, we then do, as Ian says, if you've got a website or external IP addresses which you use to remotely connect. Every month we'll do a check on those for known vulnerabilities.

And what we do find is that we pick up when people haven't configured their firewalls properly or implemented the technology correctly. And I think the fear for most businesses, they don't know what they don't know, and they automatically think it's

going to be expensive to do something about it. And there is an awful lot of free advice available in lots of different resources. And I think, just talking earlier, we were saying I don't think there's any other part of business where the government provides so much free advice to businesses to address this issue. But knowing where to find it and what the conversation is, is the challenge for any business, because they're not technologists; they're business owners and business people.

MARK COLEGATE: And Ian just a quick follow-up. One, how much capacity have you got? Because we heard earlier, actually there's probably a huge amount of underinsurance and lack of knowledge in this space. So if everyone tomorrow morning woke up and said yeah we need to get on top of this, how much capacity can you deal with? And particularly I suppose at a time, and this is the other element of it, it's some law's law of kind of cybercrime. It's AI. It seems that the barriers to entry are getting ever lower for bad faith actors to get into this system. How can you cope with all that?

IAN HICKLING: Well, I think you've hit on one point there with AI, which as you say the barriers to entry are getting much lower. We've seen that if you want to go to ChatGPT and ask them to write a phishing email and things like that, the NCSC have set up a scheme where they've had, something last year, I think it was 36 million reports of phishing emails. And I guarantee that's not all of them. But how can we cope with this? We have a growth strategy, which we'd like to take on as many businesses as possible. However, we're not going to take all of them on in one go, I mean we do have to be realistic about this, but we have plans to grow. And as long as we've got a significant proportion of businesses, we need businesses to have commercial firewall that can share that data with us. But even if they're not a member, by joining the CRC, and we're collecting enough from enough people, our intelligence picture is improved.

So even if we didn't have everybody, which would be great if we did, but I'm not quite sure the Home Office would then start to look at the cost and go how do we do it? But, as we do this, we can actually get a bigger picture of what's happening with cybercrime.

MARK COLEGATE: OK. Thank you.

STEPHEN RIDLEY: I think that's a really important part. And this idea of being able to take information from businesses and use that to inform cybersecurity posture and potentially something that's becoming more and more prevalent within the insurance space. And we do it ourselves to an extent. But what we find is that that is much less accurate, much less efficient for the smaller businesses when you're just relying on the outside in view of this. But actually having something that's freely available and is kind of plugging into the firewalls or taking specific information direct from the businesses actually (a) helps to paint a much more accurate picture, but when you've got this additional mechanism of it feeding back into that central intelligence fund that the police can then use to take other enforcement action or preventative steps in a slightly wider kind of realm than just one company at a time, to me is kind of where there's kind of a lot of the beauty of what the police are doing through the CyberAlarm. And it is why I'm

particularly so passionate about supporting both the resilience centres and the Police CyberAlarm.

MARK COLEGATE: Because you became, I think, an ambassador for the National Cyber Resilience Centre last year. So, again, what does being ambassador mean?

STEPHEN RIDLEY: So, for me, it's about, oh there's a two-prong element to it. So there's certainly the funding element. So these aren't cheap or certainly free things to put on as far as kind of the funding for it is. So, by being an ambassador, we are providing funding into that to make sure that there is some sustainability to it. But one of the things that we also see is that where customers aren't buying cyber insurance is for one of typically three reasons. It's either price, it's the impression that there's a lack of relevancy of the product or it's just an area that they see as being too complex and having too many conflicting messages around it. And when you're hearing from potentially the police, from the NCSC, from the insurance industry, from the cybersecurity industry, all with perhaps slightly nuanced messaging or things that spoken about in slightly different terminology, for me it's one of the main things we need to focus on as an industry and a wider industry.

So anyone who's working in the cybersecurity space, whether that is the insurance, the protection, whatever it is, we just need to get better at talking in really clear and consistent terms and amplifying the same message rather than just spouting out stuff that has the potential to confuse people and will be conflicting with what else is there.

MARK COLEGATE: And Ian?

IAN KIRBY: Absolutely. If I can just come in there, I totally agree that the clear and concise messaging is vital, because it's such a noisy landscape. There's information available everywhere, however that information isn't necessarily correct. And interestingly a statistic I read regarding particularly the insurance industry, which really surprised me, is that some customers who do start the process of cyber insurance, only about, apparently, 60% of those are lost along the way because it is confusing trying to fill in paperwork, etc. So if we can simplify, if we can provide consistent messaging and support small to medium businesses on their journey, that has only got to help the greater good.

MARK COLEGATE: Well, I'm going to say on that point, I mean you've made a real stress on the fact that a lot of people coming to you are not cyber experts, as firms. It's laymen with layman's language. So have you got some examples of some of the things that you can do to explain perhaps what some of the threats are, what some of the developing threats are in language that, with examples that people understand, I can see where that's relevant to my business?

IAN KIRBY: Absolutely. So we provide membership newsletters, etc., with case studies, real world examples of similar sized business in your area. Obviously these are anonymised. We would not disclose particular details. But we would use their cases, a

lived experience, to show, to demonstrate the effect of the impact and how this could happen to you. Because I think that's where the relevance comes in. But again if we go back to the consistency, so National Cyber Security Centre, or NCSC, as we know are part of the GCHQ intelligence network. They remain the technical experts for the UK. And they issue regularly threat updates on their websites, which can be quite technical.

So we provide that translation service. We stick to their advice because they are the technical authority, but we interpret that into layman's language and then deliver that at a local level so that, in bite-sized chunks so that it doesn't overwhelm, because we've all, I'm sure, got experience of those emails landing in our inbox and we just swipe, write and delete them. We deliver them in a small, easy, digestible way, again all with the longer-term view of taking that person on the journey, building their knowledge, building their general awareness so that they can help support themselves. We can't do it for them, we can't do it for everybody; it's about taking them on the journey so they understand more.

MARK COLEGATE: Thank you. Ian Hickling, I mean you talked about putting software and obviously can sort of feed back some of the stuff that's going on, the threats, some of the trends, are there any downsides for that as a business if a sort of third party software is somewhere stuck on their system?

IAN HICKLING: It's a piece of software that sits in a very, ideally it would be on what they call the demilitarised zone or secure segment of a network. And it doesn't need access to anything else on the network. All it does is collect the logs from the firewall, which is your front door which allows/disallows traffic in, passes those logs to it. We don't look at anything other than where it's coming from and the size of it and where it's going to. We don't look at the content of it. So if it was a mailroom, in would come the envelope with a ‘to address’, a ‘from address’ and we'd know the size of the envelope.

MARK COLEGATE: You’d sort of take a photo of that in layman's terms.

IAN HICKLING: Yeah and then we look at that and go is it allowed, yes/no, and your firewall says yes/no and firewall says no. We look at the outside of the envelope and that's the information we've got. So we know where it's coming from. So from that we can see sources of suspicious activity, sources of suspicious traffic, look at that and that what protocols they might be using. And what we do is we give a monthly report back to the members and try and do it in as a simple language as possible so that they can have a more informed discussion with their network manager or network provider and that sort of thing. But also it allows them to have an idea of how many times a day are they being attacked and what are the attacks, and we can see, I think with Police CyberAlarm it's the only police force in the world that's ever identified a zero day threat. Which we did with one of the particular cases, we saw a terrific spike in activity on trying to do one particular type of traffic.

I don't want to get too technical on this but basically it's like somebody coming and trying a particular window. And if everybody tries the same window, you think why are

they all trying the same window? There must be something wrong with that type of window that gets you into the network, and they look at that. And I think what we're trying to do with Police CyberAlarm is build a picture of what's happening, allow people to have the knowledge and the confidence to say well I need to get something. What are the key things I need to look at? What's critical? What's desirable? And how do we move from being down here in this bottom core tier of cybersecurity to moving up? It's like having a car or your bicycle and leaving it on the street. If you lock it up, somebody's going to sneak the next one that isn't locked.

So the idea is that you make yourself a less attractive target. This is beneficial to businesses because what it does is then demonstrates to their customers that they are a level of cybersecurity and can be trusted. And I think we're seeing this. And we're talking earlier about the supply chain, which I think is most important here, a lot of smaller businesses supply bigger businesses. Bigger businesses have massive budgets. If you were to go to any of the major retailers, they have massive budgets for cybersecurity. But the other people that feed into them are the ways in that the criminals will use. So that's why they will turn to the small/medium market and go can I get in there and force my way in through some back door into their system.

So we had an example of this, the regional airport, where there was a back door in by part of their supply chain and the whole network was compromised. They set a record of 16 what we call critical vulnerabilities, which mean there could be, they were actively being exploited. So we went down there and they turned it all off and fixed it – great! And then they did some upgrades. And then they bought the people in again and they said look you've upgraded that that's fine, now we're having some new kit. But then they copied over the old configurations and recreated the same problem again. So it's a combination of people, processes and technology.

So it's how do you move up that scale of being more vulnerable and moving to being slightly more secure, what do you do, do you train your people? And this is where the CRCs can do some of that work as well. They will provide staff training, that sort of thing. So it's trying to provide in policing an ecosystem and along with the NCSC and the advice they provide of providing the tools for businesses. The challenge for myself and Ian is how do we convince people that it's not that difficult, it can save you money, it doesn't have to be expensive, and these are the reasons for doing it. And when we partner with people like the insurance companies or people like that and they're looking at this and saying well if you've done that or you've done Cyber Essentials or you've done any of these things, it reduces the risk doesn't it. Not only reduces the risk of being a victim but the risk of the cost of rectifying it.

MARK COLEGATE: Thank you. And picking up on that, Stephen, if you've got brokers who come to you and say my client is all over this, they're part of the National Cyber Resilience Centre Group, you know, they go along to their local group. They're getting emails, they're getting involved. They've got Police CyberAlarm. What does that do to their policy, what does that do to how you have to interact with them?

Watch: Insure TV Masterclass - Cyber Resilience

STEPHEN RIDLEY: So first of all I would absolutely be encouraging all of our brokers to join up to their local resilience centre and for them to be encouraging their clients to do so. And it's definitely the type of thing that we want to look favourably on if they are engaging in that particular way. We get to formalise anything kind of properly around that, but it's definitely something that will come. At the minute, we incentivise going through the Cyber Essentials accreditation, and we do allow premium discounts based on having that certification and being able to demonstrate that you are an above average risk. And we're just working through some of the mechanics of how we can do that with the engagement with the resilience centres and the Police CyberAlarm.

Because Ian's point was exactly right, humans of all types follow the path of resistance all the time and the same applies to criminals in this space, and they will go for that low hanging fruit. So for the majority of companies it is just taking those one, two, three basic steps that just raise you ever so slightly above, can mitigate a huge amount of the risk. And it's how we get that message across in the right way and also incentivise customers to be doing that as well.

MARK COLEGATE: And I want to come back to the point that Ian also mentioned around supply chains. Obviously as an insurer you're looking not just at SMEs but mediums, even some pretty large companies. Are you seeing any evidence that big companies now are starting to put protocols in place and say if you can't live up to this, you're out of our supply chain? And a lot of this has been driven from the FTSE 100 down.

STEPHEN RIDLEY: Definitely something that we're seeing coming into play. And actually it's something that when we're underwriting the larger companies it's a type of thing that we're asking a few more questions around in terms of how do they secure their supply chain, because Ian's absolutely right now this has been a big cause of cyberattacks over the last year or two in particular where criminals are pinpointing these either single points of failure or the smaller companies that can be a route into much larger businesses. And we're seeing it come down the pipeline from the larger companies both in the sense of mandating particular security requirements. It might be a certification to Cyber Essentials or ISO27000 or things like that, but equally the mandating of cyber insurance I think we'll see come into play more and more.

And actually for SMEs there's an opportunity to get yourself ahead of the game a bit and build a bit of competitive advantage when tendering for new business by being able to, on the front foot, evidence that you're taking this much more seriously, both through the security measures that can be taken, the accreditations that can be sought, but also having the cyber insurance in place. It's easier to have it ahead of time rather than scrambling around when you're trying to sign a contract.

MARK COLEGATE: Thank you. Ian?

IAN KIRBY: Picking up on the point around Cyber Essentials and equally then moving on to the supply chain, it's a really interesting point that actually the benefit of having Cyber

Watch: Insure TV Masterclass - Cyber Resilience

Essentials or Cyber Essentials Plus means you are more secure. And then if you were going for government procurement processes etc., you are, that is part of the conditions of the government procurement process, you have to be Cyber Essentials, Cyber Essentials Plus, and again your regional Cyber Resilience Centre can help you on that journey. We do help you achieve Cyber Essentials; but not ourselves that would be through one of our Cyber Essentials partners, who we would signpost you to and again help support you on that journey.

MARK COLEGATE: In terms of Cyber Essentials I mean in layman's terms if you sort of turned it into an exam, what is that? You couldn't have been a GCSE standard at being on top of this stuff. And I just want to get some sense of the level and the amount of work that would have to go in...

IAN KIRBY: I think that's a really interesting question. I'm not sure I can quite correlate it to that. What I would say is Cyber Essentials is really quite easy for everybody to achieve. Depending on obviously the size of your network or the size of your business, but that is fairly easy to achieve. They are fairly standard processes that you would have to show that you can achieve. Cyber Essentials Plus is a step up from that. And it's a fairly large step up. It starts to speak more around your policies, processes, etc., some more stringent processes that you have to go through. But again our trusted partners in our cyber resilience centres would support you to achieve those aims. But that is a slightly longer journey and a slightly more complex journey.

STEPHEN RIDLEY: It's slightly the analogy to the exam piece, I would say that Cyber Essentials is effectively like completing a piece of coursework for your GCSE. A highly complex piece and when you get to the Cyber Essentials Plus that you have been gone and sat the formal exam and got the full certification at the end of it. You know, this isn't degree level stuff or PhD level stuff that you've got to do; it is like the real foundational level piece. And the clue's in the name, right, it's the essentials: the things that all businesses should be doing and should be attainable for all businesses, is the important thing to it. So there's no real high demand from a real technical function to this.

IAN HICKLING: And there's even a little bit before that, which is a cyber readiness thing, where you can look for free to see what sort of things you might need to do. So that's part, if you look on the NCSE website that's on there. It gives you like an intro, like this is what you will need to look at when you're getting Cyber Essentials or something like that. And that's a good starting point to say have I got most of the things covered that I need to do from a basic point of view? It's as basic as like, if you were leaving your house in the morning, you lock the doors and windows, you know. Cyber Essentials, maybe then do you put in a burger alarm and then the next thing is then do you have a ring doorbell or some other doorbells are available, of course, or install CCTV or something like that.

So you just keep ramping it up, and I think the key to cybersecurity is having a process that goes, you've got strength in depth, defence in depth. It's not just one thing and relying on one thing, because if you have the technology right, people will still try and

socially engineer around it, so you need to make sure your staff are aware of it. And that's where the CRC can help. And there's all those, and the processes are right, and that's where your Cyber Essentials gets a lot of that information [unclear 0:29:18]. What are your processes running? Simple things as basic as a disconnected backup that you can restore from is a key thing for most organisations of whether or not it's business as normal. They might lose a day because of that, but it doesn't mean they've lost everything because they didn't have it. It's as simple as that.

MARK COLEGATE: And Ian Kirby, we've talked a little bit about some of the problems that you can face, how you build up your knowledge as a business, but one thing I wanted to move on to is who are the people the other side of all this and what's their motivation? Not least because, I've forgotten who, but one of you mentioned that sometimes you can be a victim of cybercrime as a business and not know it, which sort of suggests to me that, you know, whatever they're doing inside your systems, they're not taking obviously large chunks of money off you at any point in time. So what are some of the things, what are some of the reasons that people want to get into a business?

IAN KIRBY: There's a variety of reasons and obviously your criminal intent can range all from the state threat actors all the way down, as we've already discussed, with the AI availability, that easy access now to hacking tools, making those sort of things available to the masses now. So it's a full spectrum of criminal intent. And of course I use the word criminal, it's not always criminal; there's a lot of young people out there who are honing their skills, they're experimenting, and there are safe environments to practise your skills sandbox environments, or hack the box competitions, these sorts of tools out there. But of course it's complicated, really complicated. And if I or my son/daughter walks into a sweet shop and takes a Mars bar without paying and walks out the door - other chocolate bars are available of course - they know that's theft. But if you have an interest in gaming and you find a tool online that you can knock your fellow gamer off or you can steal some of their points or their weapons that they've purchased, there's nothing necessarily that says that's illegal. But it is illegal. It's really difficult in the online virtual world to see where that line of the sand is, is where you cross over into criminality.

You mention a lot of it is financial gain. Not all of it, but the vast majority of it is financial gain. It's greed, no more complex than that. If we discount the likes of the state espionage or intercompany espionage etc. around patents and that sort of thing, that does go on; equally disgruntled employees, insider threat is one of the largest threats. When you part company, sometimes not everybody's happy about that. But equally there are vulnerabilities from, especially following the pandemic, where we all, the majority of the workforce now works from home or works remotely with a laptop, a person leaves the company. The minute that person leaves the company, have you got procedures, policies in place which means their access is removed or their laptops are returned etc. Some don't. Some still months down the line, someone still has access.

But you mentioned not necessarily seeking monetary gain straightaway. It's well documented now, a lot of cyber incidents, certainly the big ones. Threat actors can lay dormant on your network for years. I've dealt with some similar incidents myself where they were on the network for at least two years, mapping, migrating across the network, understanding, and the level of sophistication that we've got to now is they will understand your incoming, your outgoings, your regular invoices, and at some point they will then work out what money they think you can afford to pay for a ransom, for instance, and they will then at that point activate and send an appropriate financial level of a ransom. So I might get a different ransom that perhaps Stephen would get depending on the size of our company.

MARK COLEGATE: I could see two of you want to come back on this. So Stephen let's bring you in first and then...

STEPHEN RIDLEY: And there's a whole process of this as well. There's this, there can be this perception that this is like one person's carrying out all of this. And like literally one person with their hoodie on in their bedroom kind of doing it all kind of tucked away in whatever far flung country it is. But actually the monetisation is the fundamental kind of premise for all of this. But there will typically be several people within that chain, each having their role and each looking at how they can make the most money out of that particular task as possible. So you'll have these people, like initial access brokers they'd be called, where their sole job is to look at how can I gain access to a company's network? It doesn't matter who that company is how big it is they will get in, work out who it is once they're in there. They're not going out targeting specific people generally. And then once they've done that, they will sell that access on to someone else for however much they think that's worth

MARK COLEGATE: A hundred entries into a range of funds...

STEPHEN RIDLEY: That's right and they might hear it from, OK, this is a small business so I'm going to charge £10 for someone to access that one; here's a kind of really big business where you could do some serious damage so it's going to be £10,000 for that one. And then it kind of scales up from there right the way throughout the chain. So this thinking that SMEs can be immune to these because they're too small for people to be concerned about is just a myth, because all the care about is gaining access to any network. It doesn't matter from their perspective who's behind that; they can monetise it in some way.

MARK COLEGATE: Thank you. Ian?

IAN HICKLING: I was just going to say a good example of that was one we had where we were detecting a lot of, it would be in Police CyberAlarm we could detect the locality of where the suspicious activity or criminal activity is coming from, anything malicious. And first of all when we did a lot of work with schools, and you can bet your bottom dollar the local attack on a school is coming from the kids, the students. They're trying to get in. They'd want to see what they can get up to, testing their skills on that. So that's

quite good because then we can refer them to that whole programme that we have for diverting them. But we had a case where we had a lot of suspicious activity coming from the middle of nowhere in the middle of a forest. Turns out it was a saw mill. And you think well is there a criminal gang there trying to break into organisations all around the country?

As it turned out what had happened was they were actually a victim of cybercrime because somebody had broken into their network, accessed their network and was launching cyberattacks from within their network against other organisations. And they didn't even know. So they weren't a victim, as such, but they were a victim by proxy, because somebody was using, presenting to be them to break into other networks. And that was a saw mill. You know they didn't know anything about it. So we went along to them and said what's going on here, you know. We were able to find out what the issue was and what the piece of kit was that they hadn't secured.

So that's a danger for sort of small/medium enterprise. So it's not always as you say financial gain and typically they will live in there, I think those stats in 2023 was something like anything between 70, 60 days to 200 days living within a network to find out the best time to attack, and whether that is for most money or most disruption, and undoubtedly that happened with some stake actors as well.

IAN KIRBY: Friday evenings, bank holiday weekends, festive periods, they're not going to do..

IAN HICKLING: sales, in spring, in houses. That was a great one.

IAN KIRBY: That's a large one, you know, I would suggest people don't wait until Monday morning, because they know everybody comes back into work. They want to launch an incident over a weekend when minimal staff are present and then they have opportunity to run amok across the network. But of course bringing this back to SMEs, SMEs may think well that's that's not going to happen to me, you know, why would they go after me? It's not targeted; it's completely random. It’s just people, especially with the modern technology, people can just press a button and launch an attack and, as you say, Ian, that's a great analogy with the saw mill, it's not necessarily to affect that company, but they can use various companies to then launch bigger attacks on larger companies.

IAN HICKLING: Did somebody from the National Cyber [unclear 0:38:34] spray and pray, didn't they? You just go out press a button and hit anything and if there's a weakness that's where you focus and go in there. Because from that organisation you can then hide who you are and attack somebody else.

MARK COLEGATE: And if this does happen, we've talked a lot about the prevention big better than cure, but let's say something does happen I mean from your side as an insurer what are some of the things that you can do to help SMEs? Because it's it sounds

it's a percentage game so you could do all the right things and you might just get very unlucky

STEPHEN RIDLEY: Absolutely and the idea that any company of any shape or size can be completely immune to these attacks is a complete fallacy. But it's at that point of an incident happening that having an insurance policy in place then really comes into its own, because the whole point of what we're here for really is to provide that support and assistance in the event of an incident. And not only can we help to kind of minimise the costs of that, or can we bear those costs ourselves as part of that package as well. But more importantly it's the provision of the experts to come in and handle it to mitigate any longer-term impacts. And you mentioned earlier on kind of about average of £3,000 being the cost, actually from our standpoint our average claim cost last year was about £10,000, which for a small business could be a pretty catastrophic if you're at the smaller end of things. But actually 10% of our claims had a value in excess of £50,000, which again if you're a small business could be disastrous for you. But in terms of the value of the product that compares to average premiums in the hundreds or low thousands of pounds.

So actually the trade-off there is significant. But as I said it's not just the covering of those costs, it is the mitigation of the longer-term impacts. Because if you're scrambling around at the last minute having suffered an incident, not knowing how to deal with it, how best to handle things, then that can have a much longer lasting, much deeper impact. And we've seen businesses go bust because of having incidents, and largely because of how things aren't able to be handled in the correct way, whereas we're able to parachute our response teams in, who are used to dealing with dozens of these types of incidents every week and month. So they're able to navigate around them in a much more quick and efficient way.

MARK COLEGATE: So we've got a couple of minutes left but one thought that struck me as we were talking, you know, small businesses, all of the individuals, on the one hand they might be a small business owner, but they're also, they're an individual. They've got their own passwords and bank accounts and everything else. Is there a point where some of this is going to bleed across into personal insurance?

STEPHEN RIDLEY: Definitely, so we're seeing some of that come into play more so on the high net worth side of things. I think most high net worth propositions now can have some form of cyber cover within them. I think it's an area where we'll see significant more growth over the next few years, because I'm sure you guys will be able to talk in better terms than I can from the police side of things but absolutely like online fraud affecting individuals is a really, really significant issue. I just saw something online yesterday about criminal gangs, which must be UK-based as well because it's going around door to door putting through notices that look like they come from the Royal Mail with a QR code on them, trying to get people to scan those and then kind of transmitting money on the back of that. So these are kind of all different types of fraud that are being carried out and yes I think there will be a growth in the personal life space as well.

Watch: Insure TV Masterclass

- Cyber Resilience

MARK COLEGATE: Thank you. Ian, get your thoughts on that, and also as a detective superintendent I mean we see a lot of police resource directed offline, because traditionally that's where all the crime prevention needs to be. Within all of this, is the police force overall shifting and, you know, when some of these incidents go through the courts, how, you know, I mean how much deterrence is there in the sentencing, you know, people thinking actually this is, you know, I could get caught if I do this and I don't want to be.

IAN KIRBY: No, absolutely, and so there is a multiple workstreams ongoing in government of which I advise on and equally Stephen will be invited. I know there's a lot of work going on with the insurance space at the moment and a lot of the large companies are helping shape the cybersecurity strategy moving forward. The Computer Misuse Act is currently undergoing a review and that currently sits with between Home Office, Cabinet Office and the judiciary. It's recognised that, you know, the Cyber Misuse Act was written a long time ago now and there are many more named phishing attacks for instance weren't even thought about when the Computer Misuse Act was written. So legislative, legislatively-wise, that's all being reviewed or rewritten. The cybersecurity strategy is all being reviewed and now greater collaboration with industry to learn from industry how we can work collectively as part of that ecosystem to protect the UK economy.

Within policing, temporary commissioner Peter O'Doherty has recently launched the new cyber and economic crime plan. And traditionally cyber and fraud were quite separate in policing terms; they're now coming together. The City of London as the lead force for both cyber and fraud are aligning strategically and they have just launched the new economic crime and cybercrime headquarters. And again with the likes of my company, the National Cyber Resilience Centre Group there to enhance the support, the victim's support that we can give to companies to build their resilience. Hopefully, this is us doing our bit, but you're quite right, and this comes back to why it's vitally important to report the crime to Action Fraud, report any incident to Action Fraud's single reporting system so that we can understand the intelligence and the mechanisms of the attacks, coupled together with intelligence gathered from the likes of Police CyberAlarm and various other tools, such as NCSE's own early warning system, very similar product, free again from the government. We can take all this intelligence. That will then help inform our funding streams etc. to be able to deploy more officers within that space.

MARK COLEGATE: Thank you.

IAN HICKLING: We've also with Police CyberAlarm, because we know where this activity's coming from, like with the schools we know it's local, we're being able to be more proactive in that space and we just learnt earlier this week about a case where within four hours they have arrested somebody who'd been hacking into their previous employer. And that's an ongoing case there. So we're able to do that. I mean the perception always with CyberAlarm, oh it comes from abroad and nothing can be done. In many cases there are people where we can't pursue them; however, if you look back historically to Sir Robert Peel, his idea was that the policing was there to prevent crime.

Watch: Insure TV Masterclass

- Cyber Resilience

So prevention is very much part of it and the more intelligence we gather by collecting the information from things like Police CyberAlarm, people reporting things, and Police CyberAlarm is a way of reporting the unsuccessful ones without you doing anything, we can start to build a picture and help people to become better protected. And I think it's a two-prong thing. If we can deal with the people that we identify locally, we can start to make more cases, which then make the news and people start to realise it is a serious offence, and then we can also start to promote the message of prevention as well.

MARK COLEGATE: We are out of time. We have to leave it there. Thank you so much for watching. Now we mentioned a number of websites and areas where you can get help from, much of it free. We're going to make sure we've got all of those links underneath the player. Just remains for me to thank our fantastic panellists today, Stephen Ridley, Ian Kirby and Ian Hickling. From all of us here, good bye for now.

**** END OF GROUP DISCUSSION ****