[music]

Alana: Hi there, my name is Alana Muir. I'm joined with Matt Horton today. We're going to be looking at when a cyber claim becomes a D&O (Directors & Officers) claim.

Matthew: Hi, Alana, yes. There's been a lot of commentary in the insurance press about the crossover between a financial crime policy and a cyber policy. What I don't think we've seen that much of is how the management liability policy and the cyber policy interact. In the event of a claim, how does the policy respond?

Alana: Okay. Why don't we start with an SME claims example for a cyber claim, and how a cyber policy responds, and then we can look at how the D&O or policy would respond.

Matthew: Sounds good.

Alana: I had an insured where the employee received a phishing email and it manipulated them into clicking on a link which delivered malware to all the vulnerable systems. This actually gave access then for the hacker to the SME systems. In this situation though, it wasn't actually the client or our insured that the hacker was after, it was actually the insurance client's data. That's actually quite common for SMEs. What happened in this instance was they got told eventually by a third party security firm that their systems have been breached, and that's one of the worst things that could really happen from a reputational perspective. By the time they actually took the investigation piece, the hacker had left and taken the client data with them.

In terms of how the cyber would respond, initially what would happen is the client would pick up the phone, they get through to Aviva and a breach coach. The breach coach, he mobilizes all the moving parts because so many things need to happen at the same time. Initially, they'll mobilize IT forensics, they'll come out, they'll look to diagnose the source of their breach, establish how many records have been affected to help them meet their GDPR requirements, plug any gaps, or restore any data that's been lost or corrupted. Meanwhile, the solicitor will be advising them on the legal obligations for GDPR, the notification piece, not only to the regulator or regulators.

It could be FC-regulated, so it may have more than one. Then they've got to look at the regulator, they've told the regulator about it, so they'll need to defend themselves. They'll look at picking up the defence costs, any insurable fine coming from that, they may have suffered a business interruption, so as well as that, they'll have the loss of income, increase costs of working, potential loss of future custom, any extortion. As real as that, you'd also have the kind of multimedia cover to help them manage their multimedia channels as well as our PR reputation cost and experiences. That's actually how the cyber policy would initially respond. Why don't we look at what happens later when it hits the D&O?

Matthew: It's funny, because as you say all of that, there's so many little buzzwords, keywords that are coming out from what you said that would potentially trigger the management liability. You start to talk about regulatory issues. You talk about

potential for fines. Now, I think probably in terms of an ML (Management Liability) policy, in terms of D&O section, it's probably a slightly higher bar because you'd have to find that the insured person had a direct responsibility. Don't forget, of course, we've got CLL (Corporate Legal Liability), corporate legal, on the ML policy. Most SMEs buy that alongside the D&O. That's definitely going to be, at least at first instance, a cover that could trigger for those regulatory oversight any sort of fines.
You talked about reputation. That can definitely impact the ML policy across probably more the CLL again, and just a lack of confidence in the business. Think about how if you have your cyber security breached and client details are disseminated out into the world, that could impact your financials as well. When we talk about financial crime, we talk about an attack going against the cash flow of a business. Usually its cash flow that can shut a company down. If you run out of cash, it's really hard to do anything. Ultimately, with certain cyber attacks either directly or indirectly, it's a cash problem.

Then you've got the other problem as well being that the data that the company holds is so important. If you can't access your data for a period of time, then your ability to trade is diminished. Where are my D&O underwriting hat? I think, well, there's definite problems there in terms of just financial strength. It's always been the case that as the financial health of a company deteriorates, the probability of a D&O or ML claim arising increases.

Then we can talk about things like just taking the important people out of the business, right? If you think about what does the D&O section do primarily, it covers the decisions that people make running that company. First of all, are those decisions going to be compromised? Because they've got this cyber event, they're probably not qualified, they don't have a lot of experience in how they're going to react to it. Just second of all, they're making decisions that they're probably not too experienced with, and they can't make the normal decisions that they would be. They compromised individuals, at least for a short amount of time.

I think ultimately, the number one thing that gives me confidence, and I think cyber events are going to be increasing over time, is if they have a cyber policy in place, because I know, as a D&O underwriter, that if that event happens, and we get into a point probably where it's not a question of if anymore, it's a question of when it does, they have the ability to call on experts. A lot of that unsure, unless that insecurity is dealt with. You've outsourced it, you've passed it off to someone else, an expert, and they're going to guide that decision-making along that process, and with the right amount of information.

Alana: And I think, as well, because how big cyber claims can be, it’s not uncommon, particularly for SMEs, for them to get to seven figures. What SME has seven figures spare in the bank? And then, when things go horribly wrong, the first thing the regulator is going to do is look at the directors and say “right, how did you manage this risk?” “did you talk about it at every board meeting?” “what actions did you take?” and unfortunately, a lot of the time, it’s not on the agenda, or if it is on the agenda, you don’t have the proof to back up what decisions they’ve made. So basically, if it’s not written down it didn’t happen.

They also look at things like employee training, so the regulator will quite often say, “You can’t plead ignorance in this day and age” “so you’ve made a conscious decision not to train your staff,” “to protect the data within your organisation.” So that’s something else they could go after, and ultimately, one of the biggest selling points of D&O is looking after your own personal wealth. You’re only a limited company as long as you do nothing wrong!

What we're really getting at here is directors need to take cyber rescue seriously because it's going to affect the financial performance of the firm. It could be long-term, it could be short-term, it can affect customer loyalty, it can affect their brand, their reputation, without that, you know where are they? It’s one of the least well-managed risks within an organisation and it's not really that it's anybody's fault, it's just that the cyber risk domain has outpaced your traditional risks, like your financial and operational risks.

The downside to that and operating in that way as you could end up in hot water down the line. GDPR came into play, and a lot of organisations viewed that as an IT problem but actually, it looked at processes it looked at, sales and marketing, a company can't make a decision about sales and marketing without considering the cyber risk to the business.

Matthew: Ultimately, what we kind of arriving at the point of is that a well managed cyber risk by buying cover that gives you access to experts, it's ultimately going to make your the D&O and your ML a better, more attractive risk to insurers and, we've seen the the ML market, the D&O market harden massively over the last couple of years, I think we're starting to see some insurers creep in some cyber exclusions on to their a ML policies, because they probably can't get their arms around how that risk is controlled, like you said, as fast as it is evolving.

If I think about seeing a risk come through, I think probably in a short term horizon, there will be questions about how are you dealing with your cyber exposures and ultimately, the probably the number one way to deal with it is to buy cover that not only gives you indemnification, but also gives you access to people who know what they're doing in that time of crisis that can guide those directors that run the company to make the right decisions at the right time and do everything that they can to reduce and mitigate that cyber exposure and ultimately, that's going to make it a better management liability risk as well.