Why should businesses have both cyber and commercial crime cover?

Jennifer: Hi, I'm Jennifer Wells, I'm the Head of Crime. I'm here with Jake McCanney, our Cyber Trading Underwriter, and we're going to attempt to demystify the crossover between cyber insurance and crime insurance. The fraud landscape is continually changing, but what we are seeing is theft, moving away from physical means to virtual means by a computer, hence the birth of cyber insurance. So, Jake, can you comment a little bit about what's covered under the cyber policy?

Jake: One of the things that I think is a very kind of difficult challenge, particularly with cyber, is the way that we phrase cyber-crime. Because cyber-crime insinuates that we've got a lot of the cover is on that one little add-on right at the end when in reality, hacking into someone's business, whether that's for data exfiltration through ransom for extortion, anything like that is a crime. It is illegal to hack businesses, but the fact that's covered under the core covers instead of the crime, I think leads to a lot of confusion. So, the cover itself, or what cyber's designed to do in itself is its main purpose, is mainly as a service to make sure that we're protecting our customers in the event of something going wrong. Whether that's kind of a data breach, could be human error, or it could be a third party, looking to gain access to extort through phishing, whatever the circumstances are. The real kind of key aspect of the insurance is to fix that. So that's bringing in those kind of third-party experts for IT incident response, the forensics, the legal teams, the kind of notification to the ICO, the full kind of wraparound support that you get with all of our experts and then that kind of cyber-crime as we call it, which is actually just socially engineered stolen funds. It's just not quite as catchy as cyber-crime. That's just an additional aspect to make sure that we're protecting as much of the cover as we possibly could, rather than what might be a more comprehensive and rounded crime policy, which I think is something a bit different, if that's something you want to go on with.

Jennifer: So, you're right, the crime policy is much more, it's much wider, more encompassing, policy. And the crux of the cover comes in two main forms. So external crime, which you've touched on there, and the method, that's committed would be where your cyber policy kicks in. And the second element of crime, is the internal fraud element, which often gets overlooked by companies, that one of their biggest risks is their own employees. So, the social engineering aspect of cover is in the press and the news articles. I mean it's, it's relevant from a business sense, but also from a personal sense. So, there's a lot of, activity socially around how to protect yourself. So, if you migrate that towards, your company where you're working, those controls should exist there as well. So, to move away from the theft of goods and assets as a physical means, to a digital form of crime where the theft is conducted by computer means, so that will still mean the crime policy will protect the insured against loss of assets or money, but it doesn't cover the means of the attack. So, it won't cover the damage to computer systems; the hacking event itself, that's where the cyber policy kicks in. So, there is a fractional crossover of cover, but I think it's more widely expected that one or other of the policies will respond to both events, whereas that's just not the case. The crime policy really is covering the outcome of whatever cyber event that is. So, whether it's hacking or phishing or social engineering of some description, the crime policy is there to pick up the loss of actual goods or actual money, that goes missing, that is not picked

Why should businesses have both cyber and commercial crime cover?

up by the cyber policy generally. So that's really complete balance sheet protection. In a real-world situation can you give me an example?

Jake: Yeah, of course. So, I think a really good example of where there's the separation would come down to something like a manufacturer. So, in the instance that you've got an attacker gaining access via whatever means, phishing, social engineering through business email compromise, what could happen essentially if the machinery was turned off, potentially data subjects' information was released online. There's an issue in terms of getting this network back up and running as well as potentially stolen money from their own bank account. Where the cyber would kick in essentially would be that immediate instant response, getting people on the ground looking at those computer systems, making sure that those massive machinery tools which now are of all automated electric manufacturing plants would be turned back on, get that production line running again, cover the business interruption of the downtime, make sure that there's an investigation into what an attacker might have seen, what information they might have stolen, and if that information's been released. It could include the negotiation in terms of the ransom, it could include the ransom itself if the insured chose to go down that route. And what we would be doing is really just looking to get the insured back up and running and getting the stolen information back if possible, or notifying data subjects, making sure that everyone's aware of what's gone on and that there's no ongoing negative impact to either the insured, the insured's clients, or employees or whoever's information has been lost. And making sure that the required bodies such as the ICO are notified and aware of everything that's gone on. Where do you see the crime really as taking over from that?

Jennifer: So, another example would be if the intent of the fraudster was to steal money, the fraudster might purport to be a supplier, request the bank account details to be changed, and then our insured would be paying money directly into the fraudster's bank account rather than paying the supplier that was due. So essentially that's when the crime policy would be triggered. We would investigate and the funds would be reimbursed to the client as part of the claim. One key thing to remember is that the threat of the internal crime has not gone, it's just been added to by a bigger threat of external crime. So your crime policy will provide cover for both elements, the internal and the external, and we'll reimburse you for any funds lost due to fraud.

Jake: So it seems really clear that for an insured to be fully protected against crime, whether that's internal or external, online or offline, that they need to have both cyber and crime policies in place that will dovetail really nicely together and ensure that the cyber can be there to bring in that incident, immediate instant response and all the support to bring them back into place and the crime can be there to reimburse any stolen monies or lost goods.

**** END OF VIDEO****