KCS Group Europe

The third age of insurance?

March 2022

The past five years have been a minefield for insurance. First, there was the increased wave of cyber-attacks and hacks that tore up what traditional policies meant. Then, there was the coronavirus pandemic which steered the market into genuinely uncharted waters. And now, the war in Ukraine which has caused an exodus of international companies and business from Russia, and a large degree of uncertainty about what happens next. For this 'third age' of insurance problems to have hit in half a decade, the sector is going to have to face a more important reckoning than ever. Not only because of the cumulative weight of these problems, but the fact that – even in the face of anonymous hackers or a global pandemic - the Russians may arguably be the worst of them.

Until a few years ago, the biggest problem in the insurance world was what exactly could be classified as a 'hack'. All too often, phishing emails or similar that required the victim to effectively allow the compromise in the first place, by clicking the link or installing the program, did not actually involve any hacking by bad actors and so, when victims went to claim the insurance pay out, they went home empty-handed as no strict cyber-compromise had taken place. It was made plain that ransomware and its cousins that relied not on brute-force attacks, but unwitting compliance, would define the future of the insurance sector, at least in the short term. And so, it proved, until early 2020 when 'coronavirus' and 'Covid-19' were added to the collective mental dictionary, and businesses of all kinds sought to adapt to a harsh new reality. Rather than attempting to define what was worthy of insurance, or not, insurers and financial professionals were now tackling two problems: not only the severe drop-off in areas of business such as travel and establishment in new markets, but in a new frontier of exploitation and fraud that could be enacted under the guise of coronavirus-related measures. Problems arose with phantom claims, grappling with the as-yet-understood consequences of 'Long Covid' and how this would affect genuine vs false claims, and of course, the new 'Work from Home' environment having a significant impact, not only on the judging of claims, but the ability of insurers to perhaps deal with them in the first place.

Now, Russia's war on Ukraine and its global consequences look set to rip up the rulebook of insurance once again. Not only in the sense of determining the immediate impact of the initial Western pull-out and the vagaries of the fast-changing situation on the insurance market, but in the repercussions that will result from the Russian response to being cut off economically, politically, and arguably, morally, from the rest of the world. An avalanche of claims related to unexpected losses due to war, and the decreased likelihood of exposure to key Russian sectors aside, Moscow has a history of reacting subtly, yet brutally, to setbacks and responds to any perceived threat or slight, even when these are warranted. For instance, any firm still operating in the Ukrainian market, or looking to help with reconstructive efforts, would find itself a key focus for cyber attacks and compromise, while companies looking to take their business out of Russia and elsewhere are likely to be particularly targeted, on the basis that the repudiation of the Russian corporate environment is enough of a reason to prevent you from doing business anywhere else.

The challenge for insurers in this 'third age' is that it represents a melding of the worst facets of the previous two. Just like Covid-19, there is the need to respond to an unforeseen global situation that both enhances the present risk and limits the pool of new business in key areas; and just like the wave of hackers, there is the reality of facing a threat whose edges cannot be defined and whose ultimate capabilities remain unknown. Insurers should tighten up their KYC and diligence policies as a matter of course for any work emanating from, or connected to, the Russia-Ukraine war, but expand these across the board to encompass the threats from state-sponsored cyber actors working from other countries, or Politically Exposed Persons and Ultimate Beneficial Owners from Russia attempting to game the system that now seeks to exclude them. One thing that has always been clear is that the frontiers of Russian aggression do not stop at the borders of Ukraine, and their differing form makes them no less dangerous.