The Challenges of Ransom Payments and the International Sanctions Regime

Published 24 March 2022

There is growing interest in the insurance and cyber market as to the international community's implementation of sanctions in response to Russia's invasion of Ukraine. At present, the threat of a military response from Western forces seems unlikely and the reaction to date has mainly focused on methods of applying economic pressure through the imposition of sanctions on the Russian government without the use of lethal force.

As a result, a number of the new financial sanctions have created additional obligations on entities who must now ensure that they do not fall foul of the new restrictions or they risk facing severe repercussions. The newly implemented sanctions are wide-ranging and untested and this in turn has created a level of uncertainty as to their impact amongst the cyber market.

Prior to the Ukrainian invasion, a number of sanctions were already in place under English law (principally through the Proceeds of Crime Act 2002 and the Terrorism Act 2000) that prohibited the payment of funds to certain terrorist organisations or groups and individuals that were located in certain jurisdictions. Other jurisdictions have their own provisions, including, notably, the Office of Foreign Assets Control ("OFAC") of the US Department of the Treasury, and those carriers involved in the payment of ransoms have had to take appropriate steps to ensure the legality of any such payments. During this time, there were no sanctions in place that prohibited someone from paying a group or individual simply by means of being associated with the Russian state.

However, in response to the invasion by Russia, one of the many newly implemented financial sanctions introduced in the UK prevents funds or economic resources from being made available to or for the benefit of certain entities or individuals. It provides that a person must not make funds available directly or indirectly (or for the benefit of) to a designated person if that person knows, or has reasonable cause to suspect, that person is making the funds so available (individuals and entities listed on the sanction list are known as "*designated persons*"). Making funds available indirectly to a designated person includes, in particular, making them available to a person who is owned or controlled directly or indirectly by the designated person.

Consequently, the question is whether there are grounds for knowledge or suspicion that there is a sanctioned person involved in the transaction. It is important to note that it only needs to be a suspicion, which makes it a far reaching determination. Given that there is viable intelligence which shows a number of the groups and individuals responsible for ransomware attacks are based in, or affiliated with Russia (by supporting the government), there is likely to be an increasing suspicion amongst those who fall victim to a ransomware attack that they may be paying a demand to a designated person, albeit potentially indirectly.

Directly or indirectly making funds available is considered a criminal offence – in others words, a person making the payment, or the person offering to reimburse such a payment (e.g. Insurers) is indirectly making the funds available. Insurers would have an obligation to report this to the Treasury should a potential sanction be breached.

Regulators and Courts are likely to be very stringent in their approach given the obvious political pressures and those seeking to make such payments must ensure that appropriate steps are taken to ensure compliance with all applicable laws and regulations. It is very possible that parties who wish to engage with threat actors in order to minimise the financial impact to their businesses will not have that option available to them. This may mean that encrypted data for which there are no back-ups may not be recoverable, and that there is an increased risk of data publication on the dark web. This is, however, a fast moving area and further developments are expected.

Authors

Patrick Hill

London - Walbrook

+44 (0)20 7894 6930

phill@dacbeachcroft.com

Brett Randles

+44 (0) 20 7894 6377

brandles@dacbeachcroft.com

DAC BEACHCROFT