CAN TRANSNET RELY ON FORCE MAJEURE FOR ITS RANSOMWARE CYBERATTACK?

Category: Privacy Law, Infosec, and POPIA,Technology Law
written by Lucien Pierce | August 3, 2021



Transnet, on 22 July, suffered what it has called “a cyber attack”. As a result of this disruption, Transnet could not provide the services it usually provides, which include loading and offloading containers from ships. Transnet, whose ports, railways and pipelines are critical infrastructure, is crucial to the functioning of South Africa’s economy, declared force majeure on the same day as the attack. *Force majeure* is a French phrase which is typically used in a legal context. It is a clause which is usually inserted into contracts where a party is allowed an opportunity (to use non-lawyer terminology) to buy itself some time. Basically, it is given more time, beyond the agreed date, to deliver what it was supposed to, without any financial penalties or other consequences.

Traditionally, force majeure clauses allowed a party some breathing room in events such as fire, flood, earthquake (or similar elements of nature), war, insurrection (I know someone who’s now paying attention), terrorist acts and acts of God. In more modern times this has extended to nuclear explosions, sonic booms and arguably even zombie apocalypses (check out clause 42.10 of Amazon’s terms of service and tell me they’re not referring to a zombie attack).

So, in an attempt to discover what Transnet’s force majeure clause says, I went to Transnet’s various websites. Of course the claimed force majeure event, that had prompted Transnet to declare force majeure, had resulted in all its sites being down because of (you guessed it) the force majeure. However, with a bit of forensic sleuth work, and using a brilliant resource – the Wayback Machine – that archives almost every web page on the internet. I found a standard trading terms and conditions document for 2020/2021 titled Standard Trading Terms and Conditions of the Roro, Break-Bulk, Agricultural, Bulk, Ro-Ro Automotive and Inland Terminals of Transnet Port Terminals, An Operating Division of Transnet SOC Limited. With this document in hand, I made two assumptions: that the document is current (i.e. it has not been amended) and that it is the standard terms document that

Transnet gives its ports customers.The terms and conditions address force majeure at clause 11. It defines force majeure as:

"…in respect of either Party, any event or circumstance, or combination of events or circumstances occurring during the operation of these Standard Trading Terms and Conditions, the occurrence of which is beyond the reasonable control (directly or indirectly) of, and could not have been avoided by steps which might reasonably be expected to have been taken by, such Party acting as a reasonable and prudent commercial entity."

The terms and conditions go on to give examples of force majeure events which include threats of terrorism, sabotage, acts of vandalism, power failures and meteorites (almost as good as Amazon's zombie apocalypse). I considered each of the others listed in the clause, but none of them came close to including a ransomware cyber attack (assuming that the various news reports are correct).

At this point, it is probably appropriate to point out that, if you are going to regard a ransomware cyber attack as a force majeure event, it is recommended practice that you say so, unequivocally, in your contract: especially given the 485% increase in ransomware attacks in 2020 alone and the fact that well publicised ransomware attacks have happened to port terminal operators such as Maersk, since 2017.
So, is there room for Transnet to argue that this cyber attack was "beyond [its] reasonable control" and "could not have been avoided by steps which might reasonably be expected to have been taken"? Beyond reasonable control means that the situation must have made it impossible for Transnet to perform and that the situation could not have been avoided by taking steps that would reasonably have been expected of it.

Whatever the IT system was that was affected, it was certainly core to Transnet's operations. Something so important to its operations would have merited a far higher level of attention. It would have required Transnet to take all reasonable steps to ensure that it was aware of and had addressed any known vulnerabilities. News reports have disclosed that the strain of ransomware is known as "Death Kitty" or "Five Hands" and have implied that there have been similar such attacks in recent months. It appears that this is not a new strain of ransomware, with security agencies in other countries having issued warnings about it.

At this point in time, and with more details likely to be revealed in time, it is not looking good for Transnet. Even with the limited information that we have now, it looks like this criminal cyber attack could possibly have been prevented. It is also a pity that, with the huge growth in cyber attacks, particularly the ransomware kind, Transnet did not update its force majeure clause to provide for (in addition to old biblical events such as plagues, pestilence and falling meteorites) cyber attacks and other modern force majeure type events.

So, if any of Transnet's customers decide to litigate and Transnet uses the force majeure clause as a defence, my view is that it will be hearing this cyber-sound (any Pac-Man fan who grew up in the 80s, will know what it means) at the end of the court case.