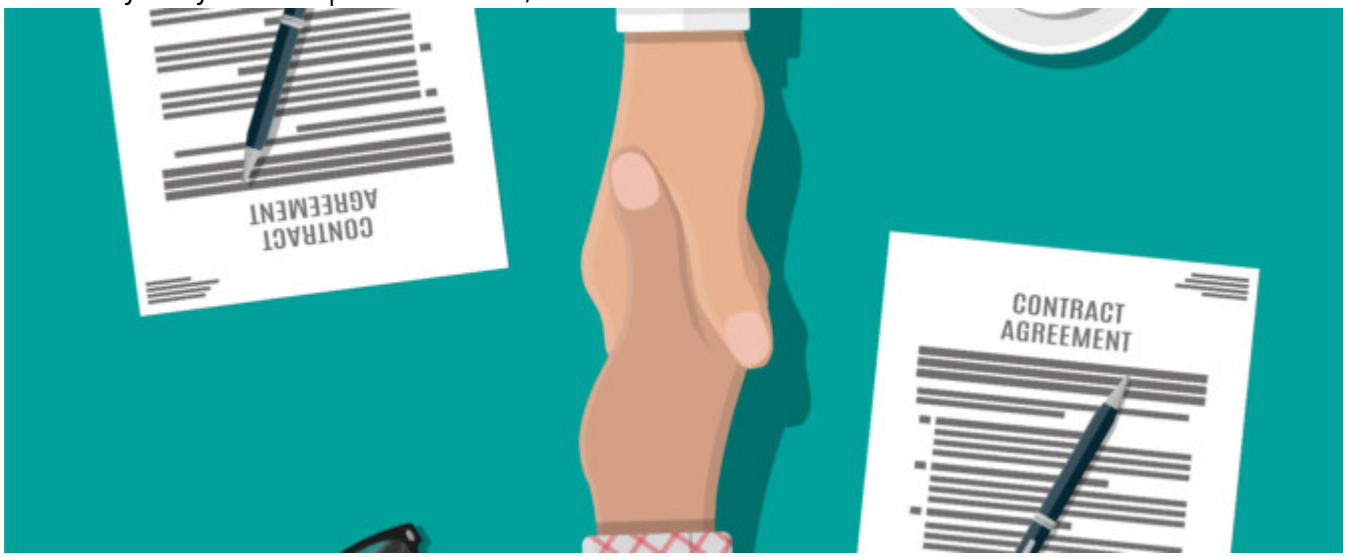
SHOULD CONTRACTING PARTIES INCLUDE A CYBERSECURITY CLAUSE?

Category: Commercial Law,Privacy Law, Infosec, and POPIA,Technology Law
written by Kelly Lekaise | November 23, 2021



Cyber attacks are fast becoming the norm in our society. The COVID-19 pandemic has accelerated this with a 485% increase of ransomware reported in 2020. A cyber attack to an organisation's system impacts more than just an organisation. The impact can extend to clients, suppliers, contractors, and employees. A cyber attack is even worse in instances where personal data is accessed and exposed. With the prevalence of cyber attacks, the question that arises is whether an organisation may contract out of liability for damages caused by a cyber attack?

Typically, parties to a contract will include a force majeure clause, which governs the parties obligations in instances where an unforeseen event beyond the parties control, that prevents them from performing, occurs. It will govern the extent to which the parties will be held liable, capping their liability, or extinguishing liability altogether. These Force Majeure clauses often cover natural disasters or "Acts of God" such as hurricanes, earthquakes, floods, and other weather-related events. It can further cover other events such as wars, terrorism, civil unrest, pandemics and fire. Because data breaches are becoming more frequent, contracting parties may consider expressly including cyber attacks or data breaches within the ambit of the force majeure clause. On one hand, a party may include a force majeure clause in order to relax the party's obligations to perform due to a cyber breach and on the other hand, where one party suffers the loss of data and the other party wishes to escape liability. In this case, a clause purporting to contract out of liability for a data breach will not hold in court, and in instances where a cyber attack results in loss of personal information, section 99 of the Protection of Personal Information Act 4 of 2013 ("POPIA") imposes strict liability upon responsible parties.

The parties can further include a cybersecurity clause. This clause would require organisations to have in place cybersecurity measures against cyber attacks, and as well as an effective system in case of breach. The clause can require the organisation to disclose the cyber breach in a timely manner, and to adhere to safety and security practices as far as reasonably possible. It can further place a threshold for recoverable damages in the case of breach, thus not extinguishing liability. Holding organisations liable will also result in firms taking cybersecurity seriously and ensuring that there are security measures in place to prevent cyber attacks. Ultimately, this will increase client trust and facilitate the free movement of information between client and organizations.

In conclusion, to ensure that there is no confusion regarding liability in the event of a cyber breach, parties should include a cybersecurity clause to govern any breach. The more common cyber breaches are becoming, the more parties should plan accordingly, not only with their internal strategies to minimize cyber breaches, but also in contracts with third parties that will provide certainty in the form of a cybersecurity clause.

Contact us for more good, clear, precise advice.