Further information surrounding the specific details and extent of the security breach suffered by transport and logistics network Toll, which we previously blogged in respect of, have been revealed by the Australian Financial Review.

The crippling ransomware attack, known now as “Mailto” or “Kazakavkovkiz” caused Toll to suspend many of its delivery and tracking systems with a Toll spokesperson indicating that the company needed to suspend up to 500 applications that supported its operations across 25 countries worldwide. In Australia, entities such as Nike, Optus, and Telstra were forced to address a multitude of customer complaints arising out of packages affected by the relevant cyber attack.

Toll has indicated that services are slowly being reactivated with core systems being tested, restored and operating as normal, and that it is working with experts from the Australian Cyber Security Centre to work out how to further respond in the most effective manner. However, a significant portion of the damage has already been done, with the article advising that Telstra and Optus have had to make new agreements with Toll’s commercial rivals and refusing to comment on whether they would resume services with Toll following resolution of the relevant breach.
What is apparent is that these sort of events can happen to nearly any business and the impact is significant. This makes it a Board level issue to ensure system resilience.