Monday, June 15, 2020

On Tuesday last week, Lion Beer Australia announced it had experienced a cyber incident. During the week, Lion advised there was no evidence to date of any data breaches, but was still investigating the cyber attack. Investigations revealed Lion was subject to a ransomware attack.

Lion shut down all of its systems as a precautionary measure, which caused disruption to its suppliers, customers, broader supply chain and brewing process.

The timing of the cyber attack and resulting disruption to Lion’s business has come at a terrible time. Lion acknowledged that the attack “could not have come at a worst time... This has been the most devastating time on record for the hospitality industry”.

As COVID-19 restrictions begin to ease, the hospitality industry in Australia and New Zealand are in the early stages of re-opening its doors. Lion’s cyber attack has impacted pubs and clubs trying to recover, restock and rebuild following the COVID-19 restrictions.

The cyber incident highlights the disruption an attack can have on supply chains and customers already struggling due to the health and economic impacts of COVID-19.
Lion’s cyber incident is a timely reminder of the importance of staying vigilant and protecting your business against cyber attacks, especially during the COVID-19 pandemic.

Steps businesses can take include updating data breach response and business continuity plans to address the unique challenges of operating in a COVID-19 world, implementing multi-factor authentication for your systems and cloud services, especially remote access systems and ensuring systems, such as VPNs, firewalls and the most recent security patches are up to date.

Copyright 2020 K & L Gates

Source URL: https://www.natlawreview.com/article/d-oh-beer-company-suffers-cyber-attack