THE
NATIONAL LAW REVIEW

Cyber Attacks Becoming Common Place: Different Industries, Similar Methods

Monday, February 25, 2019

Popular car manufacturer Toyota has been hit by a malicious attack rendering their employees completely unable to access their emails. It is unclear whether any customer or employee data has been accessed, and Toyota is going to extensive efforts to discover the origin of the attack.

Staff who are powering on despite their access restrictions have been told to use face-to-face, phone and text communication until the emailing system is back online. Can you imagine!

Although the central server system is inaccessible, dealerships are continuing to operate normally besides being able to provide customers with the date they'll receive their exciting new car.

Article By K&L Gates
Cameron AbbottCyberwatch: Australia

Communications, Media & Internet
Corporate & Business Organizations
All Federal

Additionally, Melbourne Heart Group was subject to a cyber attack which completely locked them out of their filing system. 15,000 files were scrambled and held for ransom after a cyber crime syndicate hacked into their server, blocked all access to files and demanded a cryptocurrency payment be made.

Melbourne Heart Group is based at Cabrini Hospital in Malvern, but the separation of their systems ensured that no Cabrini operations were affected. Even though a payment was made to decrypt their servers, information including patient details and sensitive medical records are yet to be recovered.

Payment in these situations is always troubling, dealing with faceless individuals, having to trade in cryptocurrencies in order to chart a course to the fastest resolution.

Ella Richards contributed to this post.

Source URL: https://www.natlawreview.com/article/cyber-attacks-becoming-common-place-different-industries-similar-methods