

### **Business interruption**

A food trucking company suffered a ransomware attack where cybercriminals encrypted all of their data files and requested a ransom of \$9,920 in exchange for the decryption key. Like many modern companies, their entire business was run via their systems and hackers had encrypted every single piece of data that they required to run their operations – their routes, logistical information, key contacts, and how much stock they had and needed to order – as well as shutting down their payment card processing capabilities.

Even though business had come to a halt, the CEO refused to give in and pay the demand. Instead, the company immediately set about reconstituting data from a collection of paper records and their employees' knowledge of day-to-day operations, resulting in a large amount of overtime costs right away. What was worse, however, was the loss of business income that resulted from the extended outage of their systems and the consequential impact on operations.

For the month of November, the insured had forecast that they would complete 220,000 sales transactions but, due to the system outage, they were only able to process around 140,000. With an average transaction value of more than \$12, that was a loss in revenue of nearly \$1 million. After adjustment by their cyber insurance provider, the insured was able to recover nearly all of the financial loss suffered under their policy.