Case study

# Database debacle

## A ransomware attack throws up unforeseen complications for a domestic goods retailer

Over the past two decades, technology has transformed the way businesses operate, and most depend on their computer systems in one way or another. Even traditional businesses, such as retail stores and wholesale distributors, utilize computer systems and the data held on those systems to ensure the day-to-day running of their operations. If those systems become unavailable or cease to function properly as a result of a cyber attack, it can have a detrimental impact on the business in question and result in substantial financial harm.

One of our policyholders affected in such a way was a home improvement store, which operated from a single store. The store sells a wide range of domestic goods, including outdoor furniture and sheds, garden equipment, kitchen utensils, bathroom fixtures and fittings and DIY tools and equipment. Customers can buy in-store or have larger items delivered to their houses upon request. The business has a large warehouse connected to the retail store which is used to store stock that can then be used to replenish stock on the shelves, or in the case of larger items, brought out for customers to collect or have delivered.

## Did you know?

A ransomware incident is not always as straightforward as decrypting systems and automatically regaining system access. There can be a number of unforeseen complications, including total or partial data corruption.

## Employee falls hook, line, and sinker

The incident began when an employee fell for a phishing email. The email stated that there was a financial statement attached that needed to be verified. Even though the email was not directly addressed to the employee, had numerous grammatical errors and appeared to come from a suspicious email address, **curiosity got the better of the employee and he clicked on the attachment.** Upon clicking on the attachment, a ransomware variant was downloaded onto the business's server and began encrypting files and programmes across the network, including the insured's back-ups, which had not been stored externally.

With the server encrypted, the business wasn't able to access any of the systems that it used every day, including the point-of-sales system and information relating to sales, deliveries and stock management.

**Urgently needing to regain access to these systems and databases, the policyholder reported the matter to CFC's cyber claims and incident response team.** With the insured's back-ups having been encrypted by the ransomware, our claims and incident response team considered the other options available. The first step was to establish which ransomware strain had been used in the attack by looking at the ransom note and a sample of encrypted files. In this case, the ransomware used was a well-known and well-established strain and the team was able to find a freely available decryption key online. Using the decryption key, the team began the process of decrypting the business's programs and files.

In most cases involving ransomware, once a business's data and programmes have been decrypted and the ransomware has been removed, the business can continue to use its computer systems as normal.

However, things aren't always as straightforward as this. Unfortunately, cybercriminals don't have the same approach to product due diligence that law-abiding businesses do, and those who create ransomware won't have gone to the effort of testing how compatible their ransomware strains are with every conceivable type of file or program. As a result, **ransomware can lead to unintentional and sometimes irreparable damage** to electronic files and computer programs.

In this case, although the majority of the business's data was accessible following the decryption process, **a database containing six months' worth of information relating to stock levels and delivery statuses was corrupted.** In spite of numerous attempts to reconfigure and restore the database, the files were deemed to be beyond repair, rendering them inaccessible to the business.

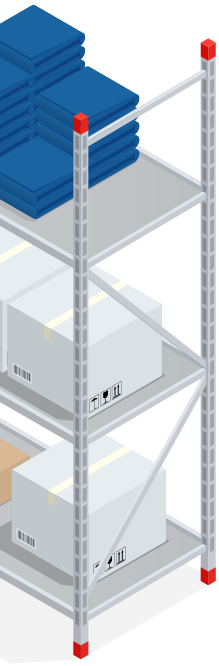
## Corrupted database causes long delays

Without access to the database, the business faced numerous difficulties. Staff on the shop floor were unable to check the most up-to-date database to see if a particular item was in stock. So in the event that a customer asked if an item was available, the only option was for a member of staff to contact a member of the warehouse team and ask them to trawl through the warehouse to see if the item was there, leading to significant delays to the service. **The lack of information on stock levels also meant that the business didn't have an accurate overview of which items were low in stock and needed to be re-ordered from suppliers,** resulting in a shortage of popular items. In addition, without access to delivery information, the business lost track of the delivery status of certain items, which resulted in items either not being delivered to the customer on time or in some cases being delivered twice.

The only way to tackle this issue was to manually re-create the current stock inventory. In order to do this, employees had to go through each item in stock, both in the warehouse and on the shop floor, create an identification number for each item and then scan it back onto the database. The business also needed to gain a better understanding of the delivery status of all items. To avoid delays and duplication, staff were required to go through all open sales and see how these corresponded with hard copies of delivery receipts to establish which items had been delivered and which items were still awaiting delivery.

Given the size of the store and the amount of stock and sales data this involved, this was a significant undertaking and staff were required to work overtime, but this alone wasn't sufficient. The business also had to bring in contractors to assist with the task. In total, **it took two weeks for the business to fully rebuild this database.** This came at a cost of $20,858 made up of employee overtime and contract staff costs.

Although the store remained open during the entirety of the recovery period, **disruptions to the service did result in a reduction in sales.** For the month in question, the business had forecasted sales of $460,031, but the actual sales for the month only came to $353,611, a shortfall of £106,420. Applying a rate of gross profit of 20% to the shortfall, the insured's business interruption loss was calculated at $21,284.



## The role of human error and other lessons

This claim highlights a few key points. Firstly, it illustrates how human error plays a key role in many cyber incidents. Lots of businesses refuse to buy cyber policies on the basis that they have good IT security in place. But **this reasoning doesn't take into account the fact that the majority of cyber incidents are the result of human error.** In this case, the incident was triggered by an employee clicking on a malicious attachment. Businesses should look to ensure that employees are educated about the risks posed by phishing emails and are made aware of how to spot them.

Secondly, it highlights how dealing with a ransomware incident is not always a straightforward matter of carrying out the decryption process and the business in question automatically regaining access to their systems and data. **In reality, there can be all sorts of unforeseen complications.** In this instance, even though the data and applications were decrypted using a freely available decryption key, the ransomware itself had corrupted one of the business's key databases, which had a detrimental impact on the insured's operations.

Thirdly, it demonstrates the importance of having data re-creation cover on a cyber policy. Many cyber policies only provide cover for the costs to recover or restore from back-ups, but not the costs to re-create or re-enter lost data from scratch. A sizeable portion of the insured's claim came about from **the labour costs associated with staff and contract workers having to manually scan and re-enter data** to ensure that the stock inventory was correct and up-to-date, and brokers should be sure to check that their clients have this important cover in place on their policies.

Finally, it reveals how almost all modern business have some form of cyber exposure. Even though the business in question was a household goods store that did not solely rely on its systems for the business to operate, **the business still relied on its computer systems and data to manage the store effectively and to provide efficient customer service.** When some of the business's data was corrupted, it had a negative impact on overall operations and having a cyber policy in place provided a valuable safety net for the company. ●