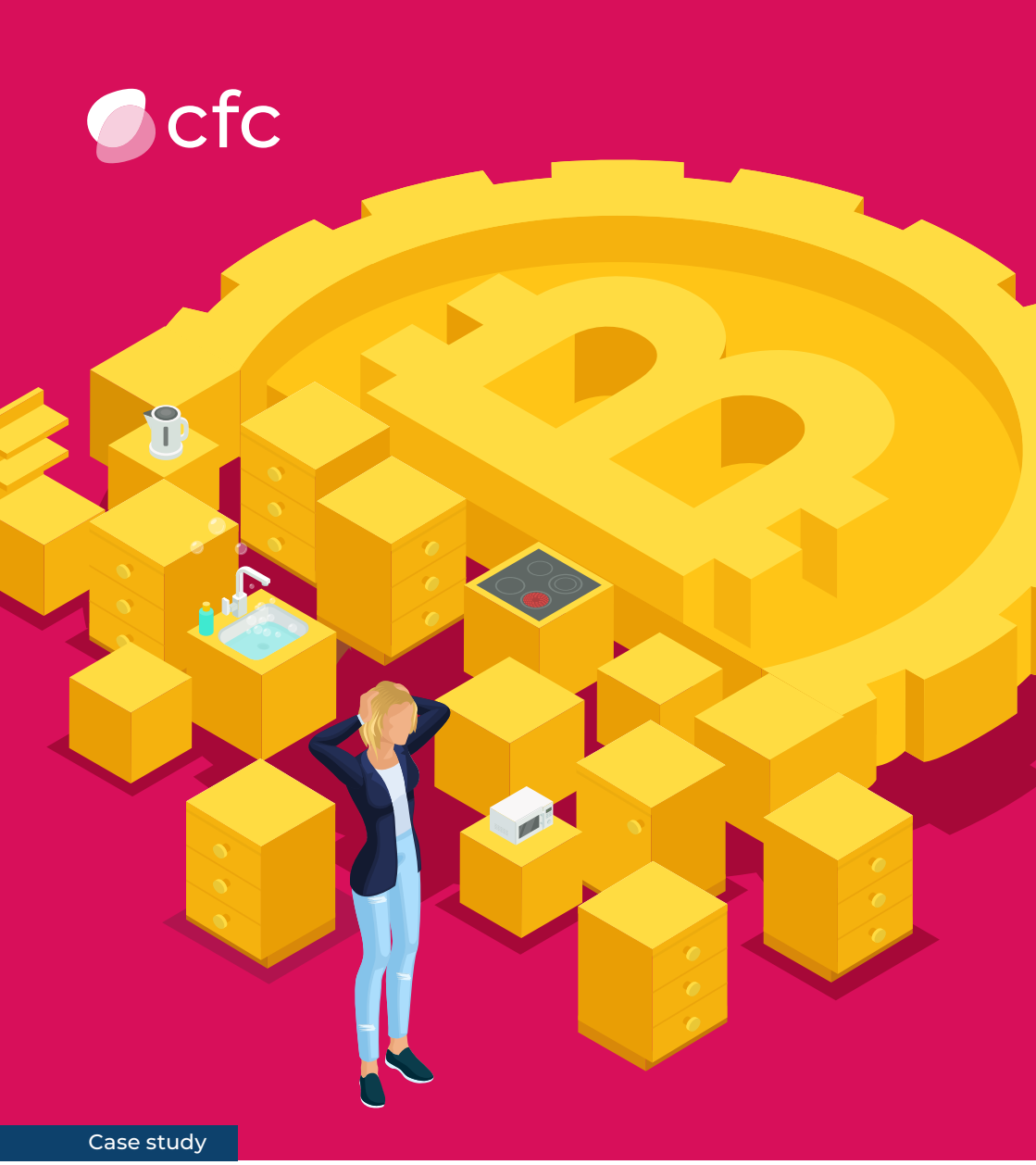


Case study

Kitchen calamity

A kitchen unit manufacturer shelves several days' profits after ransomware attack

Relative to many other industries, manufacturers have historically been slower to purchase cyber insurance policies. Because they typically don't hold large amounts of sensitive data, and as cyber policies have until recently been seen as being focused on protecting against the risk of a data breach, manufacturers often don't believe that they are overly exposed to cyber risk.

However, most modern organizations will utilize their computer systems to perform certain key business functions in one way or another. Should those systems become unavailable as a result of a cyber attack or a system failure, it can have a detrimental impact on the business in question and result in substantial losses being incurred.

One of our policyholders affected by such a loss is a medium-sized manufacturer of kitchen units, specialising in providing bespoke pieces for the residential property sector. Although the majority of the workforce is engaged in the manufacturing process, the company also employs a sizeable number of sales and admin staff who rely on their computer systems to arrange appointments, produce quotations and keep in contact with prospective customers.

Firm's security comes unhinged after brute force attack

The incident began when a hacker managed to gain access to the firm's computer systems through the Remote Desktop Protocol (RDP). RDP allows remote users to connect to the desktop of another computer through a network connection and is typically used by organizations **to allow employees to access their networks while they are away from the office**. In this case, the port that the insured used for RDP access was exposed directly to the internet rather than using the more secure connection provided by a virtual private network (VPN).

Having identified this vulnerability, the hacker initiated a brute force attack to obtain the credentials to the local administrator account. A brute force attack is where a hacker uses a computer programme to crack passwords by trying every possible password combination in rapid succession. Unfortunately, **the local administrator account had a weak password in place**, and it didn't take long for the hacker to gain access to the account.

Once the hacker was logged in, they then downloaded software that allowed them to obtain the insured's domain administrator account credentials, allowing for **greater access across the network**.

With these credentials at their disposal, the hacker then went on to launch their encryption software across multiple servers, leaving a ransom note for the insured and requesting that a payment of 3 bitcoin be made in return for the decryption key. Having discovered the ransom note on Monday morning and realising that they were unable to gain access to their systems, the business attempted to restore the servers from back-ups. However, it transpired that some of the back-ups had not been saved externally and thus had also been compromised by the attack, meaning that they would be unrecoverable unless the ransom was paid.

After this initial delay, the business notified CFC's cyber incident response team. The team quickly engaged one of our specialist partners who got in touch with the hacker, paid the ransom and decrypted the affected servers within three days. Despite the quick response, **the insured still had four working days without full access to their computer systems** and this had a deleterious effect on business operations. Although the ransomware attack did not have any impact on the machinery used in the manufacturing process, it did cause significant problems for the insured's sales and administrative functions.

No system access sends business operations awry

The policyholder's business model essentially works by having prospective customers contact the admin team, either by phone or email, to enquire about getting a quote. **The admin team then use a CRM system to take a note of customer contact details** and arrange a time for a salesperson to visit the customer. During the appointment, the salesperson will ask the customer what they are looking for, take some measurements, and afterwards produce a quote.

To produce a quote, the salesperson will use computer aided design (CAD) software to create a range of possible designs to help the customer visualize how the kitchen units will look, as well as providing some pricing options. If the customer chooses to go ahead with the quote, the salesperson will then send the selected design over to the manufacturing team. **These kitchen units are made to order**, so nothing is produced until a confirmed order has been received.

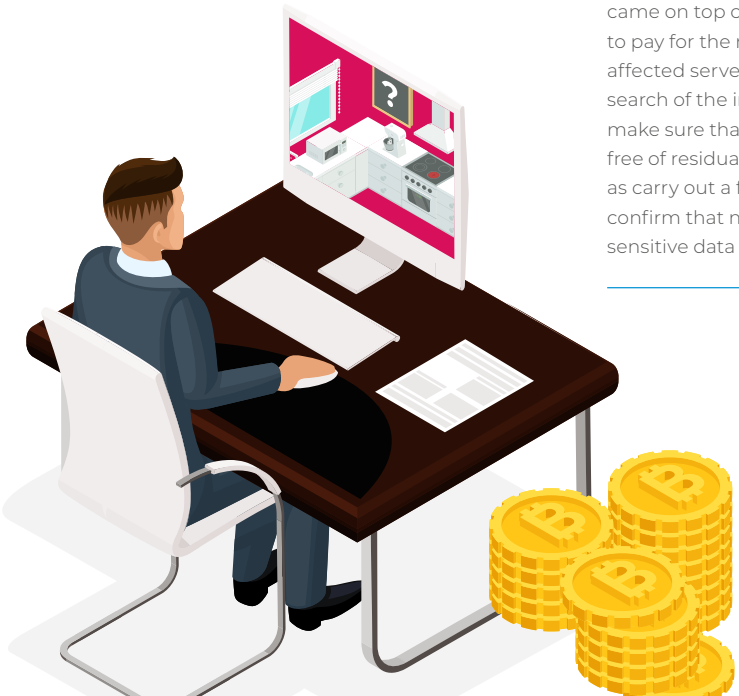
With their computer systems down, however, the business faced numerous difficulties. For a start, sales staff were unable to utilize the CAD software that they use to produce quotes, so it wasn't possible for them to finalize the designs that they had been working on prior to the attack. In addition, sales staff couldn't gain access to their emails or the CRM system containing customer contact details and were thus unable to respond to customer queries or contact them to chase up on pre-existing quotes.

What's more, the admin team was unable to access the CRM system to arrange appointments and so any new customers that called up were told that the company was experiencing technical difficulties, with admin staff having to take a note of customer contact details by hand and let them know that they **would get back to them once the computer systems were back up and running again**.

Given that the business works on a made-to-order basis, the manufacturing side of the business was also affected. With no new orders coming through, the manufacturing team could only work on those orders that had already been made prior to the ransomware attack, resulting in a significant drop in output.

Lost business and staff overtime racks up costs

When the computer systems were restored, the sales team were finally able to finish the quotes that they had been working on and **the admin team tried to arrange appointments with those prospective customers who had left their contact details during the downtime**. Even though there had been a delay, plenty of customers still chose to arrange appointments and go ahead with quotes, and this meant that the manufacturing team had to deal with a sudden influx of orders, which required staff to work overtime to help clear the backlog.



Nevertheless, many other customers explained that they had decided to take their business elsewhere due to delays in getting quotes and arranging appointments. This meant that despite managing to catch up on some of the work lost during the downtime, the insured's projected sales figures were down considerably for that month. The insured had budgeted for $2,356,000 in sales for the month in question, but they only achieved sales of $2,072,540, a shortfall of $283,460. After applying the business's rate of gross profit of 46.2%, this resulted in a business interruption loss of $130,959. This came on top of the $38,371 incurred to pay for the ransom, decrypt the affected servers, conduct a thorough search of the insured's systems to make sure that they were clean and free of residual infections, as well as carry out a forensic analysis to confirm that none of the business's sensitive data had been accessed.

System access is critical for manufacturers and most other modern businesses

This claim highlights a few key points. Firstly, if businesses are using the Remote Desktop Protocol, then they should make sure that it is not exposed directly to the internet and make use of a virtual private network (VPN) instead. **Malicious actors are constantly seeking out vulnerabilities to exploit**, and an open port used for RDP is one of the most common that they look out for. In fact, the majority of the ransomware claims that CFC has seen in recent years are a result of hackers gaining access to policyholders' systems via RDP ports that are directly exposed to the internet. In addition, business should ensure that they have good password hygiene in place and enable two-factor authentication to reduce the risk of attacks like this from happening.

One of the biggest risks that businesses face is being unable to access their computer systems. For this policyholder, being down for just four days resulted in them suffering a business interruption loss in excess of $100,000.

Secondly, it highlights the importance of having business interruption cover in a cyber policy. For many years, cyber insurance was synonymous with privacy risk, but it's becoming increasingly clear that **one of the biggest risks that businesses face is being unable to access their computer systems**. Despite only being down for four days, this still resulted in the policyholder suffering a business interruption loss in excess of $100,000.

Finally, it reveals how almost all modern businesses have some form of cyber exposure. Even though the policyholder in this case was a manufacturer of kitchen units that didn't solely rely on their computer systems to manufacture the units themselves, they **still had sales and administrative functions that played a pivotal role in the running of the business**, and they *did* rely on these systems. The machinery used in the manufacturing process may not have been affected by the ransomware attack in this instance, but the fact that the sales and admin functions couldn't access their computer systems ultimately meant that the business missed out on opportunities and lost a substantial number of orders.