Case study

Legacy system letdown

A ransomware attack on an electrical firm sparks the collapse of a vital accounting system

Businesses involved in contracting work, such as plumbers, builders and electricians, have generally been slower to purchase cyber insurance policies. Because they typically don't hold large amounts of sensitive data and they don't usually rely on their computer systems to carry out their day-to-day work, businesses of this nature often don't believe they are overly exposed to cyber risk.

However, most modern companies utilise their computer systems to perform certain business functions in one way or another. Should those systems become unavailable or cease to function properly as a result of a cyber attack, it can have a deleterious impact on the business in question and result in substantial costs being incurred.

One of our policyholders affected in such a way was a small electrical contracting firm. One of the primary activities of the firm involves installing and maintaining electrical systems for both private individuals and companies. Aside from the front line work carried out by the electricians, they also have an office function where most of the administrative activities are carried out, such as taking calls from customers, preparing work orders for electricians on the ground, sending out invoices for work completed and preparing the business's financial accounts.

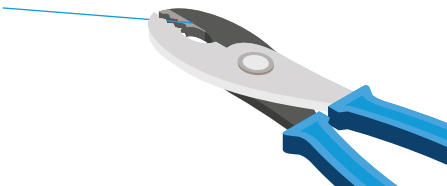
Business operations go down to the wire

Back in July 2018, one of the firm's employees received what they thought was a legitimate looking email in their inbox. The email stated that the sender was looking for a job and that they had attached their résumé for their perusal. Although the business in question was not actively recruiting at the time, the employee's curiosity got the better of them and they clicked on the attachment. The attachment actually contained a ransomware variant and **when it was opened by the employee, it encrypted all of the business's computer programs**, requiring a $5,000 ransom payment to decrypt the data.

Having realised that they were now locked out of their systems, the policyholder reported the situation to CFC's incident response team a day later. Under normal circumstances, the usual response would be to help the policyholder recover from a back-up. However, it soon transpired that this wouldn't be possible, as **the company's back-ups for the last few years had not been saved externally** and so they too were encrypted by the ransomware.

This left the policyholder with little option but to pay the ransom demand. Working with one of our partners, we began negotiations with the cybercriminals responsible for the attack, reimbursed our policyholder for the ransom payment, received the decryption key and began the process of decrypting the affected programs.

In total, this process took four days from the reporting of the incident to the business regaining full access to their computer systems again. However, this still meant that during this time the policyholder's **office staff were unable to access any of the key programs that they used on a daily basis to carry out their jobs,** and they had to resort to doing these tasks manually instead. For example, all quotes and estimates to customers had to be written down by hand; any feedback from customers or changes in their status or addresses had to be noted down by hand for future re-entry onto the insured's computer systems; all orders for new equipment from suppliers had to be filled out manually; and because the business's invoicing and accounting system was down, they couldn't take credit card payments and had to tell any customers looking to pay by this method that they would contact them at a later date for payment collection.



Faulty program leads to manual data re-entry

All of this manual processing was having a damaging impact on worker productivity and it came as a welcome relief to the policyholder when the decryption process was completed and access to their computer programs was restored. However, this wasn't the end of the matter. Although the decryption process had been successfully carried out, **not all of the insured's computer programs emerged unscathed from the attack.**

The firm had a legacy system in place, which they used to create all of their work orders for electricians and invoices for customers, as well as being used for the maintenance of the business's accounting records. Even though this program had been decrypted and was accessible by employees, **the ransomware attack unintentionally resulted in serious issues with its performance.** For example, tables were missing headers and were not formatting correctly; numerous records were corrupted or duplicated; figures were randomly changing on accounting documents; and error messages were constantly popping up and preventing work from being saved. Worst of all, the program was now running extremely slowly. Prior to the ransomware attack, for instance, it would only take a minute or so to run off a report from the program, but after the attack, it could take anywhere from ten minutes to half an hour.

Despite numerous attempts to restore functionality to the program, it was still not operating effectively more than a month after the attack. And **this was resulting in numerous problems for the business**, such as a lack of accuracy in financial reporting, a significant dip in productivity for the processing of work orders and invoices, as well as a general reduction in the ability to provide prompt and effective customer service.

Thankfully the business had maintained paper records for the data contained on the affected program and so the decision was taken to abandon the legacy system and move over to a new program instead. In order to do so, employees were required to work overtime to

manually re-enter data from the paper records onto the new program, amounting to some 1,562 hours in total. **The business also had to hire in a number of temporary employees to assist with this data re-entry work**, amounting to a further 521 hours spent on this task.

The cost to carry out this major data re-entry task came to some $58,887. This came on top of the $22,500 incurred to deal with the initial ransomware incident, bringing the total claim costs to $81,387.

Even though this program had been decrypted and was accessible by employees, the ransomware attack unintentionally resulted in serious issues with its performance. For example, tables were missing headers and were not formatting correctly

Even traditional businesses often have a cyber exposure

This claim highlights a few key points. First, it illustrates how dealing with a ransomware incident is **rarely a simple matter of the ransom payment being made 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 case, even though the ransom payment was made and the system was successfully decrypted, the ransomware had the unintended side effect of severely impairing the functionality of one of the company's most vital systems.

Secondly, it shows how the use of legacy systems can significantly increase the risk of a cyber loss. Generally speaking, l**egacy systems are not only far more vulnerable to attack, they are also much more susceptible to dysfunction following a cyber attack**. Had the policyholder been using a more modern program, the impact of the ransomware attack would most likely have been much less severe.

Thirdly, it demonstrates the importance of having data re-creation cover on a cyber policy. Many cyber policies only provide cover for the cost to recover or restore data from back-ups, but not the costs to re-create or re-enter lost data from scratch. The bulk of the costs attached to this claim came from the labour costs associated with manually re-entering data, and brokers should be sure to check that their clients have this important cover in place on their policies.

> Legacy systems are not only far more vulnerable to attack, they are also much more susceptible to dysfunction following a cyber attack

Finally, it reveals how **almost all modern businesses have some form of cyber exposure**. Even though the policyholder in this case was an electrical contracting business that didn't solely rely on their computer systems to carry out work, they still had an office function that had a key role in the running of the business. When the computer systems in that office were affected by a cyber event, it had a negative impact on the overall business operation and having a cyber insurance policy in place provided a valuable safety net for the company.