Case study

Software shutdown

Cyber attack results in contractual complications for property management firm

Cyber insurance policies have historically offered relatively short indemnity periods under the business interruption section. While traditional business interruption policies connected to property damage typically offer 12, 18, 24 and even 36 months as standard, many cyber policies only offer a 3-6 month indemnity period.

In part, this stems from an assumption that a system outage caused by a cyber event will be shorter lived than the effects of a major property damage loss. However, **it is becoming increasingly clear that the operational impact of a cyber event can be felt for much longer than a 3-6 month period would allow for.** Indeed, any cyber attack that significantly impairs a business's ability to perform a service to their clients over the longer term can result in customer dissatisfaction and, ultimately, significant financial loss.

One of our policyholders affected by such a loss was a property management company. Alongside building maintenance and administration, their service includes the preparation of monthly financial reports for their clients.

Ransomware leads to service slowdown

In late September 2017, the company fell victim to a ransomware attack that disabled their server and a number of computer workstations. Unfortunately, their data back-ups were also kept on this server, meaning that these were also impacted by the ransomware and rendered inaccessible.

Our policyholder engaged their IT vendor to fix the problem, and they quickly went about wiping the ransomware from the server and restoring the computer systems as best they could, allowing the organisation to regain access to their server within a couple of weeks. In spite of this, though, they still faced a number of complications.

Their data back-ups were also kept on this server, meaning that these were also impacted by the ransomware and rendered inaccessible.

One of the major problems for the business was in relation to their main software programme used for producing their customers' financial reports.

This software programme had been in use since the business was founded over two decades ago and included bespoke features that had been designed at the outset to help deal with each customer's data and reporting requirements. Prior to the cyber incident taking place, the business had recognised that the software was becoming increasingly outdated, and a decision had been made that over the course of 2018, the production of financial packages would gradually be migrated to a more modern system. The intention was that this would be done in such a way that the transition could be completed in normal working hours with no disruption to the service provided to customers.

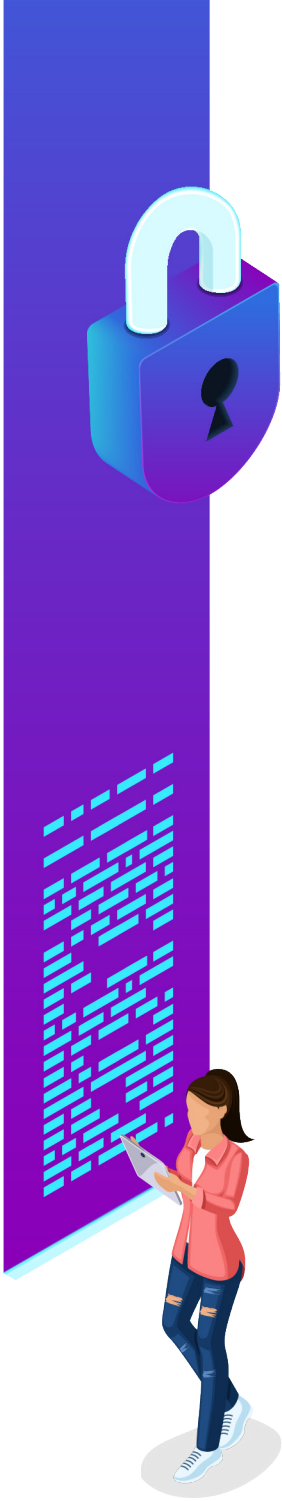
When the attack occurred, the organisation had been in the process of planning this migration. **But the ransomware spelled the end for the old software programme:** although the IT vendor managed to reinstall it, the software was so archaic that it wasn't possible to restore it to its original functionality and it was no longer capable of ▶

producing the financial reports in an effective manner. **This meant that the insured had little option but to massively accelerate the implementation of the new software system,** but they faced difficulty here too.

Because the back-ups had not been saved externally from the server, it meant that these were lost when the server was wiped. With the data back-ups unrecoverable, the insured didn't have access to the electronic customer data necessary to complete their clients' financial reports on the new system.

Thankfully the insured had retained paper copies of this information going back many years. However, in order to have sufficient information to allow figures to be reported for both current and prior financial years and for long and short term trends to be shown in the monthly reports for customers, several thousand lines of data per client needed to be manually entered onto the new software.

In order to rectify this situation, **the business had to get staff members to work overtime** to carry out the data re-entry and accelerate the software implementation. They also had to bring in a number of temporary agency staff members to assist with these tasks.



Calculating the cost of customer dissatisfaction

Even with all this overtime and external assistance, though, it still took over four months to get the new software system ready. During this time, our insured was still manually producing monthly financial reports for their clients, but this was a time-consuming process and resulted in delays to the service. What's more, because they could not make use of the bespoke software features offered by either the old or new software, **the reports that were produced were of a lower quality than their customers had come to expect.**

Despite explaining to their customers that there would be delays and a temporary blip in the quality of the reports until the new software system was ready, four months of sub-standard reports understandably led to dissatisfaction with the service. As a result, seven customers chose to cancel their annual contracts with the insured and take their business elsewhere. For this small business, **these seven customers represented nearly a tenth of their overall customer base by numbers.**

All of these customers sent individual letters to the organisation, explaining that the reason they were cancelling their contracts was due to delays in the service and the financial reports no longer meeting their expected standards. This served as confirmation that these customers were lost as a result of the cyber attack as opposed to regular customer churn. The total ▶

Client	Contract value p/a	Contract period	Amount payable over 12 month indemnity period
Client A	$32,805	1 Nov 17 to 31 Oct 18	$29,030
Client B	$50,640	1 Jan 18 to 31 Dec 18	$36,350
Client C	$8,327	1 Jan 18 to 31 Dec 18	$5,977
Client D	$46,462	1 Mar 18 to 28 Feb 19	$25,841
Client E	$35,058	1 Apr 18 to 31 Mar 19	$19,487
Client F	$14,590	1 Apr 18 to 31 Mar 19	$8,114
Client G	$5,280	1 May 18 to 30 Ap r19	$2,054

value of these annual contracts came to $193,142. As some of the contract dates did not fall neatly within the 12-month indemnity period, this meant that the overall claim size was reduced proportionately, and the loss payable for these lost contracts came to $126,853. In addition, a further four customers requested rebates from the insured for those months in which only lower quality reports had been produced, which amounted to some $14,318.

Unlike the annual contracts, the rebates all fell within the year-long indemnity period and so these costs were picked up in their entirety. **These financial losses came on top of the $94,083 incurred** to engage with consultants to deal with the cyber incident and the extra expenses needed to hasten the implementation of the new software system and carry out the data re-entry.

The value of longer indemnity periods and other lessons learnt

This claim highlights a number of key points. **First, it underscores the value of longer indemnity periods.** The reputational impact of the cyber event in this instance was not felt until after the 3-6 month indemnity period that you would find on many cyber insurance policies. Even though the cancelled contracts were not covered in full, if the insured had only had a 3 month indemnity period, they would not have been covered at all, as all of the cancelled contracts fell outside of this period. Those businesses that receive their income on a contractual basis could be more exposed to business interruption losses, as the cancellation of monthly or annual contracts could very quickly result in sizeable financial losses being incurred. Accordingly, businesses that receive their revenue in this way should consider factoring this in when selecting an appropriate limit for their policy.

> This claim underscores the importance of longer indemnity periods

Second, it illustrates how important it is to make sure that back-ups are saved externally from the main server. In this case, although the insured had been prudent enough to back-up their data, keeping it on their main server meant that when the server was encrypted, the back-ups were as good as useless. This also highlights the significance of having cover for data re-entry on a cyber insurance policy. Some policies will only cover the costs associated with restoring from back-up, which was not an option for the insured in this instance, but thankfully the costs of data re-entry were picked up under their policy.

Finally, this claim shows how the impact of a cyber event can vary from business to business. The fact that this business was reliant on a legacy system to produce financial reports meant that they were especially exposed, as it soon became clear that it was no longer possible to restore their antiquated software package and resume their normal service. Other businesses might have had their server encrypted in just the same way, but if they were using modern software packages they would most likely have recovered much more quickly.