evolve

Case study

Payroll pandemonium

An HR service provider loses contracts due to a cyber attack suffered by one of its supply chain partners

Over the past two decades, technology has transformed the way businesses operate, and most now depend on their computer systems in one way or another. Rather than having to deal with everything in-house, many businesses choose to outsource elements of their IT infrastructure to third party providers, whether that be in the form of website hosting, data storage or application level services.

In many cases, outsourcing IT can prove to be a more efficient and cost-effective way of doing things, with businesses benefitting from the expertise of their third-party providers. However, outsourcing is not without risks. In a cyber insurance context, dependent business interruption describes a situation in which a third-party organization that supplies a policyholder with goods or services is affected by unexpected downtime as a result of a cyber event or system failure. Even though the policyholder's computer systems may not be directly affected by the incident, the loss of the goods or services provided by the third-party can still have a major impact on the insured business's ability to operate effectively. This means that a business can still suffer a business interruption loss even when its computer systems are unaffected.

One of our policyholders affected by this type of loss was a small company providing outsourced human resources services to a variety of different businesses. The organization provides a range of services to its customers, including payroll processing, employee benefits and health insurance and assistance with compliance and regulatory issues.

Third-party downtime, first-party problems

Our policyholder provides its payroll processing services through an online application, which in turn is owned and hosted by a third-party provider. Their customers gain access to the payroll application through a link on their website, which then takes them through to a landing page hosted by the third-party where they can then log into the application. Once these customers log in to the application, **they are effectively operating on the third party's computer systems**, even though their contracts are with our policyholder.

The issue began when the third party responsible for providing the payroll processing application was hit by a ransomware attack. This ransomware attack managed to encrypt the servers hosting the application, which meant that neither our policyholder nor its customers could gain access to the application. As the application was hosted by this third party, however, **our policyholder was powerless to control the situation and had to rely on the application provider to respond to the incident.** The only thing they could do was to explain to their customers that the application was unavailable due to a cyber attack affecting the application provider and that regular status updates would be provided. ▶

Did you know?

Last year, ransomware and extortion was the cause behind 17% of the cyber claims our incident response team dealt with, but accounted for 33% of the overall financial losses, making these attacks disproportionately costly.

▶ In the meantime, the third-party provider went about trying to deal with the issue by decrypting the affected servers, removing the ransomware and returning the application to its normal functionality. After three days of downtime, it looked as though the issue had been resolved and the insured and its customers were able to log into the application once again. However, this breakthrough proved to be short-lived.

During the encryption process, **the ransomware had damaged the application and impaired its underlying functionality.** This meant that while customers were able to log into the application and view employee data, they were unable to update the data or process any payments.

To remedy the problems caused by the ransomware, **the application was taken down once more** and it was only after a further five days of downtime that the application was fully restored. To make matters worse, the downtime occurred at the end of the calendar month, a time during which most of our policyholder's customers would ordinarily pay their employees.

Frustrated customers lead to lost contracts

With the payroll processing application rendered inaccessible as a result of the ransomware attack, **some of our insured's customers were unable to pay their employees on time.** Although they were able to pay them once the application was up and running again, the delay in payment was a source of great frustration for both the businesses and employees affected. As the customers that were impacted only had contracts with the insured rather than the application provider, **it was the insured that bore the brunt of this anger.**

In the end, eight customers chose to cancel their contracts and take their business elsewhere. All of these customers sent individual letters or emails to our policyholder, explaining their reasons for cancelling. In each case, these cancellations came down to a combination of two factors: firstly, the delay in paying employees as a result of the ransomware attack and, secondly, a concern that the ransomware attack meant that sensitive data stored on the payroll application might not be secure.

This served as confirmation that these customers were lost as a result of the cyber attack as opposed to regular customer churn.

The total value of **these annual contracts came to $72,554** and despite the insured's attempts to placate these clients and win them back, unfortunately none of these customers decided to reinstate their contracts, meaning that over the course of the 12-month indemnity period, the insured suffered a business interruption loss of $72,554.

While these losses are potentially recoverable from the application provider, this can be a costly and lengthy process and in the meantime the insured would suffer from cashflow issues due to the drop-off in income. Fortunately, however, **the income loss from these cancelled contracts was covered under the dependent business interruption section of the company's cyber policy with CFC**, which covers business interruption losses arising as a result of a cyber event or system failure at a policyholder's supply chain partner.

Dependent BI and other takeaways

This claim highlights a few key points. Firstly, it underscores the importance of having dependent business interruption cover in a cyber insurance policy. Some cyber insurers will only provide cover for business interruption losses as a result of cyber events that directly affect an insured's computer systems. However, in this instance, at no point were the insured's computer systems directly impacted by the ransomware – it was the application provider's computer systems that were affected – and yet it still resulted in a sizeable business interruption loss. **By having dependent business interruption cover in place, the business was able to fully recover its financial loss.**

Secondly, it illustrates the value of longer indemnity periods. Many cyber insurers only offer 3 to 6-month indemnity periods as standard. However, this ignores the fact that the financial impact of a cyber event can be felt for much longer than a 3 or 6-month indemnity period would allow for.

In this case, **the cancellation of annual contracts meant that for each cancelled contract, the insured lost 12 months' worth of income.** By having a 12-month indemnity period in place, they were able to reclaim quadruple the amount that they would have been able to claim on a policy with a 3-month indemnity period and double the amount they would have been able to claim under a policy with a 6-month indemnity period.

Finally, it highlights that **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 cyber policy. ●