Case study

Reputational repercussions

Online retailer grapples with data breach aftermath

Businesses are increasingly dependent on their computer systems to perform critical elements of their operations, so it comes as no surprise that financial losses due to system outages are becoming both more frequent and severe. This has made business interruption cover an increasingly important part of any cyber policy. However, brokers and their clients shouldn't focus solely on system outages when it comes to business interruption.

Often referred to as reputational harm, business interruption as a result of a data breach is starting to impact many organisations and can be equally as disruptive as a system outage. In such cases, even though an insured may not have suffered any meaningful system downtime, they can suffer serious reputational harm in the eyes of their customers and suppliers, resulting in a subsequent drop-off in income. For instance, in 2013, the US retail giant Target was the victim of a **data breach that resulted in 40 million customer credit card details being stolen**. After news of this spread, Target saw its sales fall by some 46% year-on-year in the fourth quarter of 2013[1].

But it's not just well-publicised data breaches like Target's that can result in reputational harm and financial loss. Even small companies that experience a data breach outside the public domain can be impacted by reduced customer loyalty when they inform affected customers. One of our policyholders to suffer such a loss was a small online retailer in the US, selling medical treatments and accessories.

[1]Doug Drinkwater, "Does a data breach really affect your firm's reputation?, CSO Online (https://www.csoonline.com/article/3019283/data-breach/does-a-data-breach-really-affect-your-firm-s-reputation.html).

Notification becomes necessary

In February 2017, our policyholder suffered a number of attacks on their website. The company first became aware of the issue when they received an email from the hackers that claimed that they had obtained thousands of customers' credit card details and demanded that a ransom be paid in order to prevent the data from being released into the public domain. It was at this point that the policyholder reported the situation to CFC's in-house cyber incident response team.

> The forensic consultants discovered that a database containing the credit card details of over 90,000 customers had been accessed

Our team engaged one of our IT forensic partners who quickly rectified the problem by addressing and removing the vulnerabilities and malicious code that had allowed the hackers to gain access to the insured's systems. However, in the process of carrying out their investigations into the policyholder's computer systems, the forensic consultants discovered that a database **containing the credit card details of over 90,000 customers** had been accessed by the hackers and exfiltrated from the system.

CFC engaged our specialist privacy legal team who determined that the insured was required to notify all of the affected individuals, as each of the impacted customers lived in states with relevant breach notification laws in place. The organisation also opted to provide identity theft restoration services to these clients.

By this point, the costs of IT forensics and the provision of **legal advice and breach notification services came in at just over $230,000**. Under many cyber policies, with these issues taken care of, the insurer would typically consider the matter resolved and close the claim file accordingly.

An expensive side effect

But this wasn't the end of the matter for the insured.

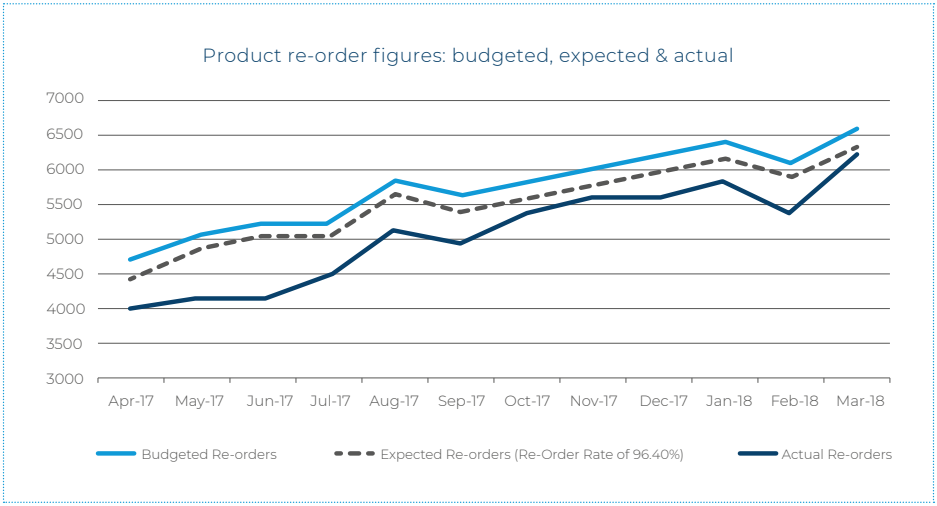
In the months following the notification, the business began to notice a drop-off in existing customers re-ordering products they had previously purchased, which was leading to a reduction in revenue and a resultant loss of profits. In order to establish the size of the loss and the extent to which it could be attributed to the notification of the data breach, CFC worked with one of our forensic accounting partners to assess the case.

As a first step, the insured put together a loss calculation based on the number of actual re-orders against their budget. It was initially established that from January 2016 to the end of March 2017 (prior to the notification), **the business had on average been achieving a re-order rate of 96.4%**. However, in April 2017 (after the notification) the figure dipped to 85.8% and **by June it had dropped to as low as 79.7%**. Thereafter the re-order rate picked up again but never returned to the established average of 96.4% during the 12-month indemnity period. After comparing the number of re-orders expected at a re-order rate of 96.4% to the actual number of re-orders over 12 months, it was determined that some 5,220 orders had been lost.

In order to corroborate the insured's estimate, the forensic accountants used an alternative approach, looking at the loss on a customer-by-customer basis. Initially, it was calculated that the insured had acquired 116,738 new customers prior to the notification but only 51,029 customers had continued to place re-orders after the notification letters were sent out, **leaving some 65,709 potentially lost customers**.

In order to deduce which customers were lost due to the data breach notification, the forensic accountants conducted an analysis of customer

> Fortunately for the insured, the cyber policy that they had with CFC covered the costs of reputational harm following a cyber event over a 12-month indemnity period



buying habits. They established that repeat customers tended to re-order every three months. If a customer did not engage in this repeat order cycle, the accountants deduced that they had been lost as part of regular customer churn. Once these customers were removed from the calculation, they were able to identify that 1,299 repeat customers appeared to have been lost in the aftermath of the data breach. As these customers were expected to re-order roughly every three months, this meant that over a 12-month period, 5,196 orders had been lost due to the data breach. Given the confluence between the insured's figure of 5,220 lost orders and the accountancy's figure of 5,196, the higher figure was decided upon as the overall loss figure.

With the insured losing 5,220 orders at a rate of profit per order of $91.12, this meant that over the course of a year, the business interruption costs associated with reputational harm came to some $475,646. Fortunately for the insured, however, the cyber policy that they had with CFC covered the costs of reputational harm following a cyber event over a 12-month indemnity period.

Reputational harm cover is key

Incidents like this highlight a few key issues. First, it illustrates the importance of having business interruption coverage in place that extends to cover reputational harm. Many cyber policies will only cover business interruption as a result of system outage. In this instance, the insured had no meaningful system outage, yet ended up with a sizeable business interruption loss due to a reduction in customer loyalty caused by a data breach.

Secondly, it demonstrates the value of having longer indemnity periods. Traditional business interruption policies connected to property damage will typically offer 12-month indemnity periods as an absolute minimum, with 18, 24 and even 36 month periods being fairly common. However, many cyber policies only offer 3-month indemnity periods as standard. In this case, had the policyholder only had a 3-month indemnity period, they would only have been eligible to claim for three months' worth of lost profits at a cost of $188,072, **leaving the insured with a shortfall of $287,574 over the course of the year**.

When purchasing a cyber policy, brokers and their clients should consider not only system outages but the whole range of business interruption exposures that they may face as a result of a cyber incident.