

Managing cyber risks Part 3: business interruption losses

Browne Baker and other key points in this series demonstrates the importance of being prepared for and knowing how to respond to a cyber incident. Part one of this series focused on the crucial role of IT contracts. Part two shows how detrimental it could be for an organization to not have a cyber liability insurance policy in place. In the last instalment of this series, learn about business interruption losses during a cyber event, and how to mitigate them.

The U.S. politician and former member of the U.S. House of Representatives, Christopher Shay, once said, "Ethics is everything - if you don't have a strong moral standing, if you don't have an ethical foundation, you just crumble."

But, just as there is a cost to business of not acting in an ethical manner, there is also a cost associated with acting ethically. Where this ethical dilemma becomes a little tricky is when the financial cost of being one of the "good guys" reaches a point where it is unclear if it is actually worth it. When it comes to ransomware, it is possible that this tipping point has already been reached.


When ransomware claims first started to occur, the actual ransom demands were sometimes as low as £10,000. However, a lot of companies, even if their backups were not complete, were not prepared to be extorted and therefore took a stand of not paying the ransom demand. This was even though the disruption to the business, in financial terms, was greater than the size of the demand itself.

Consequently, hackers have had to change tack. Now, in addition to a company's data being encrypted, the hackers will invariably have exfiltrated data which may be commercially sensitive. Even worse, the data could contain personal data, which, if it fell into the wrong hands, could be used to commit fraud.

The ethical debate has therefore changed. Does the company stand up to the hacker and not pay the ransom, thereby leaving its customers and employees exposed to identity fraud (and itself to a significant GDPR exposure) or does it bite the bullet and pay the ransom? The debate has become even more charged in the last year as the size of ransom demands have increased. For example, Acer, the Taiwanese computer company, was recently subjected to an alleged ransom demand of \$50 million.

In the case of our fictitious law firm, Browne Baker, this ethical debate will be real. As a law firm, it will hold confidential and commercially sensitive data on behalf of its clients, as well as the firm's own data. If the incident at Blue Sky, which is clearly not Browne Baker's fault, gets into the public domain, Browne Baker's clients are unlikely to have sympathy that Browne Baker was also a victim of Blue Sky's poor cyber controls. If those clients take their business elsewhere, then Browne Baker will suffer a business interruption loss. This must be weighed against the cost of paying the ransom and the time that it will then take to decrypt the data.

The good news is that cyber insurance policies provide business interruption cover that will protect Browne Baker during this period. The bad news is there is a possibility that not all losses will be recoverable under the policy.



Let's consider the short-term losses. Browne Baker's client files are stored electronically, and these have been encrypted in the attack. While some employees will have paper files and information stored offline or locally, it is likely that this will not be enough to allow for anything approaching normal work. Consequently, there will be downtime and likely a reduction in chargeable hours.

Client and court deadlines are unlikely to be altered because of the incident. Therefore, Browne Baker's restoration efforts will focus on those files with the more immediate deadlines to allow staff to catch up on the necessary work and, hopefully, still meet the deadline. In effect, those chargeable hours lost during the period of downtime will be caught up once the encrypted information has been made available again, although there is a possibility that the lost hours will not be fully recovered.

If the net total of the downtime hours and the subsequent recovery still results in a loss of chargeable hours, then the policy will indemnify Browne Baker for this loss. Similarly, if the process of catching up these lost chargeable hours means that there is an increase in overtime, then, providing that (a) overtime is usually paid to staff and (b) there is a demonstrable increase that can be clearly shown as incident related, the policy will provide an indemnity for those costs.

However, due to the issues related to the wording of the contract with Blue Sky and the lack of clear delineation of responsibilities, Browne Baker is uncertain about what data backups they have and are therefore reliant on hard copy files. The time taken to manually rebuild files is likely to be long enough to mean that client and court deadlines are missed. Depending on the nature of the missed deadline, Browne Baker could find itself subject to professional indemnity claims from clients for part of a claim being barred due to late filing.

If that happens, then in addition to the costs of defending itself against client claims, it is possible that some clients may seek to transfer files to a competitor law firm. This would have the effect of the initial post incident reduction in chargeable hours becoming a sustained reduction.

A cyber business interruption policy insures the profit and loss account for a defined indemnity period, commonly between three and six months. Therefore, the policy will provide an indemnity for whatever revenue Browne Baker would have earned from these lost/transferred files during this period. While the loss of these files will undoubtedly be due to the incident, however, any revenue losses that occur after the end of the indemnity period will not be insured. This is because it is the profit and loss account that is insured, not the files themselves.

This is not the only type of revenue loss that may occur. Before the incident, Browne Baker was tendering for a large multi-year contract with a multinational company worth £250,000 annually. However, the incident resulted in certain key documents that were needed for the final submission no longer being available, meaning that the tender could not be submitted in time. Browne Baker had reached the "last two" and the client confirmed that, but for the incident, Browne Baker would have won the contract.

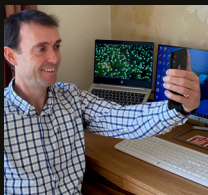
As with the lost/transferred files, Browne Baker will be able to recover some of this lost revenue under the cyber policy, but only that revenue which would have been earned during the indemnity period. Lost revenue beyond this period will not be covered.

On this basis, Browne Baker is exposed to what could be a significant uninsured loss. While it cannot recover the losses from insurers, it could, in theory, recover these losses from Blue Sky. However, as we know, the terms of that contract are such that any recovery will be extremely limited and capped to a low level of service credits. Furthermore, significant legal costs may be incurred in an attempt to argue that the contractual limitations do not apply, with no guarantee of success.

In any cyber incident, speed of recovery is essential in minimising the business interruption loss. It is likely that Browne Baker's confidence in Blue Sky's ability to provide cloud services has been irrevocably destroyed, meaning that it needs to find an alternative cloud vendor to assist in the recovery process and it needs to do so quickly. However, Browne Baker's experience of negotiating the contract with Blue Sky shows the perils of entering into a contract at haste. As the saying goes, a mistake repeated is not a mistake, it's a decision.

It goes without saying that when it comes to cyber incidents, prevention is always better than cure. But prevention means more than just stopping the hackers from getting access to the network in the first place. What Browne Baker's experiences show is that preparing for an incident and understanding how to respond is just as important to ensure that any losses that may occur can either be recovered under a cyber insurance policy or can be recovered from negligent third parties. To do this properly, though, involves more than just IT; - the issues that Browne Baker has suffered due to the incident at Blue Sky show that cyberattacks are an enterprise wide risk.

For more information on the topic, contact our authors:



Michael Ainsworth
Director
London, United Kingdom
michaelainsworth@oconnors.law



Bernard Regan, MSc, MBCS
Partner, Global Forensic & Litigation Services
London, United Kingdom
T: +44 (0)20 7065 7937
bernard.regan@bakertilly.com



Joshua Bates
Solicitor
Liverpool, United Kingdom
joshuabates@oconnors.law



Ben Hobby, FCA, Dip II
Partner, Global Forensic & Litigation Services
London, United Kingdom
T: +44 (0)20 7065 7925
ben.hobby@bakertilly.com



Kathryn Howard
Solicitor
London, United Kingdom
kathynhoward@oconnors.law

Connect with us: bakertilly.com/globalforensics
Connect with us: oconnors.law



The information provided here is of a general nature and is not intended to address the specific circumstances of any individual or entity. In specific circumstances, the services of a professional should be sought.

Baker Tilly US is an independent member of Baker Tilly International, a worldwide network of independent accounting and business advisory firms. Baker Tilly is the trading name of BTVK Advisory LLP, a Limited Liability Partnership registered in England & Wales (registered number OC304572), which is a Baker Tilly US company. The registered office is 5th Floor, 2 London Wall Place, London, EC2Y 5AU, where a list of members' names is available for inspection.
©2020 BTVK Advisory LLP

O'Connors is a trading name of O'Connors Legal Services Limited Company No. 11158860 SRA ID 647864 VAT 292977933