

# Managing cyber risks Part 1: IT contracts

**Managing cyber risk in today's world as it relates to law is vast a topic, and as such, there is far too much information to cover in one article. This article is part one of three to go over the complexities that come with cyber risk and law firms, although the issues raised apply equally to other sectors. Read part two, "cyber liability insurance policies", to learn more.**

The doctrine of mutually assured destruction has been a long-standing military strategy and a principle of Cold War nuclear deterrence. It was founded on the notion that a nuclear attack from an aggressor country would be met with a nuclear counterattack by the aggressee country, ensuring that both would be annihilated.

This apocalyptic "if I'm going down, I'm taking you with me" doctrine has arguably maintained peace since the start of the Cold War, but with an inherent flaw. If the pre-emptive strike from the aggressor cripples the aggressee's centralised command and control systems, the aggressee will not be able to retaliate in devastating kind. The need for decentralised communications systems to combat this flaw led to the proto-internet, used by universities and scientists from the 1960's to the 1980's, and then to a military-grade internet. As this internet became more widely used by the public, it emerged as the world wide web we know today.

Exponential technological advancements in the last 30 years have rapidly digitised almost every aspect of our lives, especially our work lives. There is, currently, no better illustration of businesses' dependency on technology than our collective shift to remote working during lockdown and our newfound reliance on cloud computing. In April 2020, shortly after lockdown measures were implemented globally, Microsoft CEO Satya Nadella said that the pandemic brought about two years' worth of digital transformation in two months. The scale of the swap is evidently astronomical, and it has been a large part of the survival of businesses this past year.


But have you stopped to think how resilient these cloud infrastructures are, and what would happen if another kind of virus, a digital virus, were to infect your business?

Set against the original need for the internet, it is ironic that the recentralisation of IT assets into cloud infrastructures operated by a small number

of corporations is now increasing the level of risk once again. The contracts you have with third-party IT suppliers, like cloud service providers, are the cornerstone of cyber risk management, and yet they are often misunderstood, overlooked, or just not fit for purpose. Get them wrong, and your business could be "nuked!"

In Part 1 of our cyber trilogy, we are using a fictitious law firm, Browne Baker, to highlight some of the typical deficiencies with IT contracts, and how they can have a dramatic impact on your business if these deficiencies crystalise during a cyber incident.

A cyber incident can be defined as any attempt by a third party to gain unauthorised access to a computer system's data, or use of a computer system for the unauthorised processing of data. It also includes any attempt by a third party to make unauthorised changes to the firmware, hardware, or software of a computer system, or to create malicious disruption or denial of service. In other words, it's a cyberattack.



So, picture the scene. In response to lockdown, our fictitious law firm Browne Baker has successfully managed to move all their employees to remote working. To enable this to happen, Browne Baker has engaged a software-as-a-service cloud services provider, Blue Sky, to provide storage of its historic and future data, its case management and time recording system and its accountancy software. Under pressure to continue working, Browne Baker's managing director (MD) gives Blue Sky's standard form of agreement a quick once over, signs it, and then authorises the migration of all Browne Baker's IT assets into Blue Sky's cloud infrastructure.

Unbeknown to both parties, a cybercriminal identifies weaknesses in Blue Sky's security, and encrypts Brown Baker's data with ransomware so that Browne Baker cannot access its information or use the cloud software.

As Browne Baker's MD fruitlessly tries to send an email to her employees about the system failure, she again casts her eyes over the contract Browne Baker has with Blue Sky, expelling a deep sigh as she reads that:

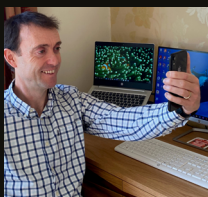
- There is no **disaster recovery** plan scheduled to the agreement and Blue Sky does not offer supported recovery strategies. What's more, Browne Baker has not updated its IT disaster recovery plan since migrating wholesale to the cloud.
- Blue Sky's **service levels** for system failures are not adequate. There is a commitment by Blue Sky to use reasonable endeavours when responding to cyber incidents, but precisely what they will do and when they will do it is not clear. Browne Baker has the right to terminate the contract for a breach of service levels, but that will not help them now, especially when it could take weeks to re-tender for a new service provider.
- The agreement specifies that Blue Sky processes data **outside of the EEA** and it is silent on the **appropriate safeguards and security measures** that are put in place to ensure compliance with the General Data Protection Regulation (GDPR).
- The responsibility for **data back-up and restoration** rests with Browne Baker, who are not sure what data has been backed up, when the back up last happened, and how it could be used to restore anything. Browne Baker is left with hard copies of their old files and no way of accessing their current client information.
- Blue Sky's **liability for indirect losses is excluded** and all other loss and damage is **capped at a low level of service credits**.

The combination of these issues leaves Browne Baker in a cyber quagmire - unable to return to operations (even at a reduced level) and reliant on the goodwill of Blue Sky for help. Browne Baker is also facing difficult conversations with the Information Commissioner's Office and the firm's clients. It is significantly financially exposed, and with little hope of any meaningful recovery from Blue Sky.

The deficiencies highlighted above are common in IT contracts and we are all guilty on occasions of skipping the small print and signing the terms and conditions presented to us. Even where the terms and conditions cannot be negotiated fully, as may be the case with large IT service providers, a thorough understanding of them should leave you better informed and better able to take other steps to manage your cyber risk, including transferring some of the risk to cyber insurers.

**Continue reading our managing cyber risk series in the next article “cyber liability insurance policies”.**

**For more information on the topic, contact our authors:**



**Michael Ainsworth**  
Director  
London, United Kingdom  
[michaelainsworth@oconnors.law](mailto: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](mailto:bernard.regan@bakertilly.com)



**Joshua Bates**  
Solicitor  
Liverpool, United Kingdom  
[joshuabates@oconnors.law](mailto: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](mailto:ben.hobby@bakertilly.com)



**Kathryn Howard**  
Solicitor  
London, United Kingdom  
[kathynhoward@oconnors.law](mailto:kathynhoward@oconnors.law)

Connect with us: [bakertilly.com/globalforensics](https://bakertilly.com/globalforensics)  
Connect with us: [oconnors.law](https://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