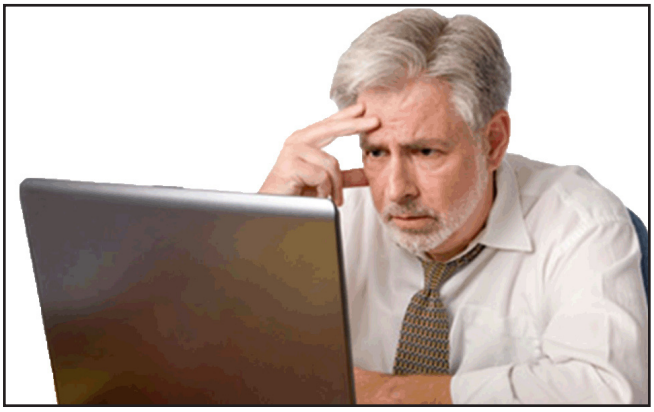
Fields **Associates**
Litigation Consultants

Speak directly to a qualified member of staff
0845 301 5778

You may never have heard of it, but a form of computer virus known as ransomware could cause vast and irreparable damage to your business. What's more, a greater number of these viruses are now active than ever before and it's been estimated that their popularity amongst cyber-criminals grew five-fold last year

Ransomware is essentially a type of Trojan horse virus which, once it has found its way onto a hard drive or, worse yet, server, will proceed to encrypt all of the data stored there before demanding a substantial fee for the decryption key. These viruses quite literally hold your data to ransom, hence their name.

Such viruses have grown in popularity thanks to the success (for want of a better word) of CryptoLocker, a particularly efficient and unpleasant type of ransomware that has been used to fleece thousands of pounds from unsuspecting and unprepared individuals and businesses sine it first emerged in the middle of 2013.



Previous forms of ransomware were, fallible meaning that experts were able to find ways of decrypting the data that these viruses had scrambled. CryptoLocker, however, is robust and, in spite of continued research, those that are unfortunate enough to be affected by it have two choices: pay for the decryption key or lose data. To the consumer, ransomware is a significant threat. To businesses, it is something far worse.

From spreadsheets of clients to financial information, the data held by businesses is now, more often than not, amongst their most valuable assets. Should a type of ransomware find its way onto your servers, all of this vital data will be encrypted within seconds. At worst, this could cripple a business and will, at best, cause significant disruption. Even if the company were willing to simply bite the bullet and pay for the decryption key, this will still bring about hours of downtime and the resulting financial losses will be significantly greater than the outlay required to regain access to your data in the first instance. On the other hand, should you refuse to pay the ransom, then your expensive equipment such as servers and other forms of storage media will be rendered completely useless. Fortunately, with a few simple steps, you can significantly negate such risks.

The first thing that you must do is ensure that your employees are advised not to open suspicious looking emails or open any attachments from people they do not know. Ransomware is commonly spread via email so this is absolutely essential. Secondly, ensuring that all vital data is backed up to drives that are not attached to your network is equally vital and will allow you to create a viable contingency plan in the event of drives failing for any reason; not just ransomware. Ultimately, with robust and well-thought out security measures, the threat of viruses, and many other common causes of data loss, can be avoided.

-ooOoo-