System lock out – another firm falls victim

What's your plan if you suddenly find you can't access your information on your computer? Following on from our last blog about a recent law firm cyber-attack, we bring you a different story this week.

On a recent Monday afternoon, a small firm suffered an attack on their local server which hosted their practice management software. The firm's local server was hit with three different 'infections' in the space of eight seconds resulting in a complete shutdown barring access to everything on their practice management system. The infections came via remote access. While the firm had some virus protection in place it was not enough to stop this new sophisticated attack.

They called their IT people in as soon as the attack happened. They estimated it would take at least a week to recover the system and recommended a ransomware data recovery expert be brought in. The firm followed that recommendation and it took eight days to recover the system. The cost to the firm was $30,000.

They had no **cyber insurance** to cover this. Fortunately, the firm's document management system and email were on a cloud server and unaffected. The experts also determined there was no data accessed or lost on the local server.

While it took a week to be back to full functionality, particularly for time recording and billing, the firm was able to complete multiple settlements during that time in accordance with contractual requirements — although it took a lot more time and effort to do it.

Interestingly, there was no ransom demand, as is usual in an attack resulting in a system shutdown. The experts suggested it might have been an attack by someone who was just testing vulnerabilities to see if they could do it.

The attack has prompted a rethink and resetting of priorities by the firm for dealing with the threat of cyber-crime. The firm had a mix of internal and external IT assistance and have now decided to outsource all their IT support to a specialist cyber security organisation that can monitor and maintain their system's security.

They realized that in the current environment it is now essential to retain security experts to protect their information systems, their clients' data and their workflow operations. It is simply a core part of conducting a business safely.

As we highlighted in our last blog, no firm is immune from attack, and even the most diligent firms can suffer cyber-attacks. It is important to be taking proactive steps to mitigate the risk of an attack, such as the steps in our **last blog**, but it is also important to have an incident response plan with access to skilled cyber experts and **cyber insurance** if the worst happens.

For more information and resources to help keep your practice secure visit our **cyber security page**.

lplc.com.au/cyber