LEGAL PRACTITIONERS' LIABILITY COMMITTEE

25 October 2019

Cyber strikes again - how one small firm got hit

What's your plan for when, not if, a cyber incident occurs in your firm? There is a new phishing email scam widespread in the legal sector right now. Here's what happened to a small Victorian firm in the last few weeks and how they handled it.

A partner in the firm received an unusual email from a lawyer in a Victorian firm that he knew, but the contents of the email appeared to be from an organisation the partner had never heard of or had dealings with. The subject line was titled: 'Electronic remittance payment/advice receiver agreement'. The content in the email said the sender had sent the recipient some files which could be accessed by clicking on a link to download a PDF document.

The partner was overseas at the time and sent the email to his personal assistant (PA) to investigate and determine if any action was required. It was at this moment that suspicions about the provenance of the email were raised, but instead of calling the sender to enquire about the email, the PA clicked the 'DOWNLOAD ALL' button taking her to a website pretending to be an Office 365 site, where she was prompted to enter her email address and password to download the document.

When she entered her details an error screen appeared. The PA assumed there were no documents available and moved on to the next task. The partner didn't follow it up as he had received an email from the law firm sender saying the previous email was spam and just ignore it.

What the PA failed to appreciate was that she had just disclosed her password to cyber-criminals enabling them to access and control her email account. They did just that, and sat in the background for three weeks watching activity in the email account. Having found no money transactions to intercept, they then launched a spam attack sending a similar phishing email from the account to over 500 recipients, being contacts and other email addresses harvested from the account.

Some recipients were suspicious and replied by email querying the firm, only to receive an automatic response from the cyber criminals confirming it was legitimate. The firm was also inundated with phone calls from many of the recipients, which immediately put them on alert that there was a problem.

This was a small firm with limited resources or expertise to deal with a crisis like this. They contacted LPLC for guidance and were immediately referred on to relevant legal and technical cyber experts to help them respond. The experts directed the firm to disable the email in the administration portal on Office 365 and physically disconnect the computer. This closed off the cyber criminal's access.

Further investigation showed the PA's email had been accessed from many locations around the world with the last one being in London just several hours before the firm discovered the issue. The cyber criminals had deleted all the emails they had sent from the account and the audit setting in Office 365 had not been activated, so it was difficult for forensic experts to determine who had been emailed.

The firm is now having to undertake a laborious, expensive and uninsured process to ascertain the extent of any data breaches and re-secure their network.

What can be done to avoid something like this?

- Train staff to be suspicious and don't click on links unless sure of their legitimacy. A phone call here would have avoided the problem.
- Don't put your email and password details into a website unless you are sure it is legitimate. Be wary of impersonations of common-use platforms like Office 365.
- Use an advanced spam filtering tool – this may well have stopped the initial phishing email from reaching the partner's email account.
- Turn on multifactor authentication for accessing email accounts. This would have prevented the cyber criminal from accessing the email account from other devices — even with the password.
- If you think your email account has been compromised, immediately seek expert cyber security advice about the steps you need to take. Simply changing your password might not be enough if there is malware installed on your computer that allows the cyber criminals to track your key strokes and decipher your new password.

- Even if changing your password locks the cyber-criminals out of your email account, they may have already harvested your email contacts which they can then use to send further phishing emails from a spoofed address. You will need technical advice to work out what the cyber criminals have done. We can refer firms insured with LPLC to relevant cyber security experts.

- If using Office 365, ask your email account administrator to check and turn on the audit setting to enable you to track activity in an email account later, even if the emails have been deleted. If using other email systems look for similar settings. With this setting on you will be better able to track what client data has been compromised.

Cyber-attacks are a fact of modern life and all sized firms are at risk. We have been notified of several instances of spam attacks, phishing emails and ransom attacks on law firms in the past six months. Everyone needs to be vigilant about what they open and click on and have good systems in place and a plan for when something goes wrong.

Firms of all sizes should seriously consider the purchase of cyber insurance in addition to the professional indemnity insurance with LPLC mandated by law. LPLC has worked with Marsh Insurance Brokers who have arranged a cyber insurance policy tailored to the needs of law firms whose professional indemnity insurance is placed with LPLC. A detailed explanation, FAQ's and other information about the Marsh/Chubb cyber insurance policy can be accessed at:

lplc.com.au/cyber-insurance-cover .

lplc.com.au/cyber