LPLC LEGAL PRACTITIONERS' LIABILITY COMMITTEE

Risk video bites

Risk video bites – Cyber security

Presenter: Matthew Rose

Cyber security is everyone’s responsibility, no matter the size of the firm or your role within it. Many firms, including sole practitioners, have reported cyber-attacks to LPLC and we have received several claims.

Cyber-attacks can threaten the security of your clients’ confidential information and prevent you from providing legal services to your clients. They are disruptive and can even be destructive to your business. If you are not already taking cyber security seriously, now is the time to do so.

In one claim, a fraudster hacked into the email account of the firm or its vendor client and then monitored the conveyancing transaction. Before settlement, the fraudster sent emails to the firm purportedly from the client asking for money to be transferred to accounts that were different to the one previously specified by the client. The firm was duped into transferring the money. On closer inspection, the emails contained some red flags such as American phrasing, a different font and salutations that differed to those previously used.

We’re seeing that emails from fraudsters are increasingly sophisticated and convincing, better mimicking the style of the purported email sender.

In other instances, a hacker gained access to a firm’s email account and sent scam emails to thousands of people blocking up the firm’s email account with thousands of bounce-back and reply emails.

There has also been a growth in scams where a fraudster ‘spoofs’ an email from someone in authority to a colleague with a request for money or information.

Many firms have also told us of falling victim to a ransom attack, where a hacker installed malicious software that would only be removed once the firm paid a sum of money.

The common thread to these attacks is a hacker has been able to infiltrate a firm’s computer system, often though a staff member clicking on a link in an email. Which goes to show that the weakest link in the cyber security chain is us.

To strengthen your firm’s cyber security you need to:

- ensure your staff have regular cyber-security training
- use a business-grade hosted email service with quality filtering
- use a DNS-based website filtering service
- install reputable security software on every computer in your firm

- backup all files using an automated daily service
- keep all software up to date
- ensure all staff change their passwords at least every 12 months
- use passwords that are at least eight characters long, and contain capital letters and numbers.
- And most importantly, have a protocol in the office that all email instructions to pay money are confirmed by speaking to the client using a known phone number.

If you don't know how to implement these measures, consult an IT expert.

You can find more guidance including a cyber security checklist on LPLC's website. The Law Council of Australia's website also has useful information for firms on how to combat the growing risks of cyber-crime.