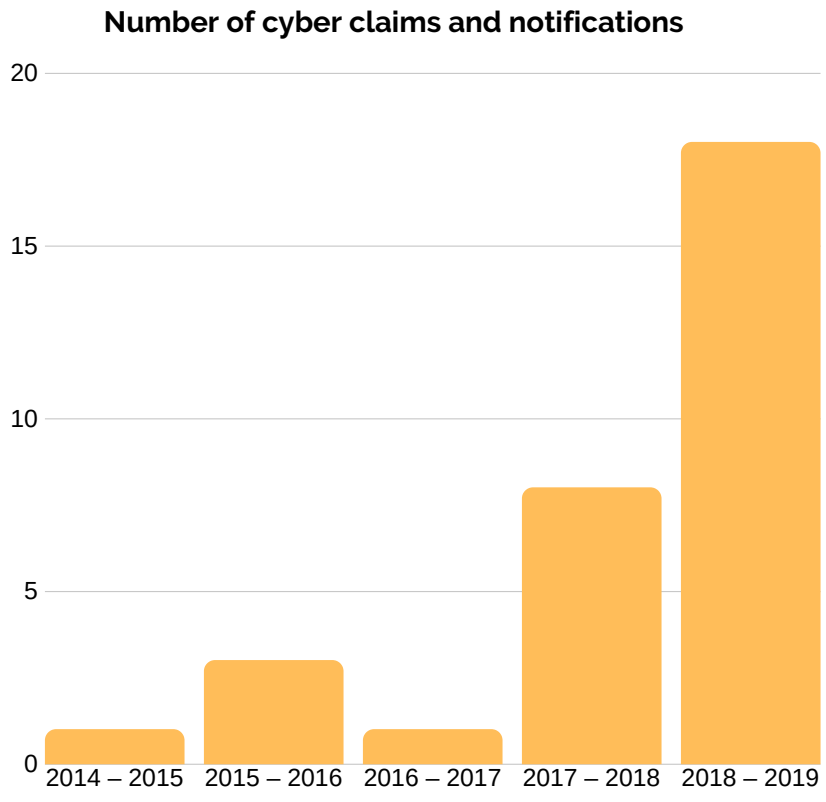
Bulletin
September 2019

Cyber claim dramatic increase – everyone is at risk

LEGAL PRACTITIONERS' LIABILITY COMMITTEE

Cyber security is an increasingly significant issue for law firms of all sizes and practice areas, it is not just conveyancing practices at risk, every practice area when they handle money is a potential target.

In the 2018-19 year we have seen more than double the number of cyber claims and notifications than the previous year, and more than the last four years combined.



The gap between cyber claims has dramatically shortened. There is more of them, happening in quick succession.

Not just a conveyancing risk

The claims we have seen have occurred across all firm sizes and locations – city, suburbs and country. While the majority occurred in conveyancing matters, we have also seen claims in family law, estate matters and several in litigation.

Some firms already have good processes and policies in place in their property department to make sure they verify bank account details sent by email. However, those firms have been caught out when another department that deals less often with client money weren't aware they needed to verify the email instructions for EFT payments.

Any time you handle money for clients you will be at risk. Any time you ask your client to pay money to you, either for a transaction or just to pay your bill, they may be at risk.

Case study

In one recent case this happened in the firm's litigation department. They received bank account details by email for the settlement proceeds to be paid. The clerk didn't call the client to verify the bank account details even after receiving a call from their accounts department to check the account details were right.

Over $1million was paid to the fraudulent account.

Fortunately, due to the fast work by those involved the account was frozen in time and the money recovered, underlying the importance of a fast response. This was a good outcome – many are not.

Five steps to protect yourself

Our **Don't fall for it** poster last year listed the five things you need to do.

Download

The most crucial step is verification.

Call the sender personally to check authenticity. Use a number you know, not one suggested in the email. Ask for the account number, write it down, then compare with the email.

Every person in your firm needs to know they must call before they pay or authorise payment of money. Give your clients this message too because many of our claims notifications involve clients receiving fraudulently altered emails and paying money to the wrong account.

We have created an email footer image available to download and use on all your email footers.

Download

The consequences of not making the call

Ask yourself this question: how would you feel if you didn't call to verify bank account details, and the money was sent to the fraudster?

- ·Practitioners have said things like 'I was absolutely horrified', 'this was the worst experience in 45 years of practice'.
- At best your client's transaction is delayed while everyone tries to get the money back. This can take some time and is very stressful for you, your client and the other parties to the transaction.
- Your reputation is damaged as your clients trusted you to look after their matter professionally.
- A negligence claim or professional conduct complaint may be made against you.

- There is a potential for a double excess under your policy of insurance if a claim results from a misdirected EFT payment. To emphasise the importance of always verifying payment instructions, LPLC's 2019/20 policy wording was changed to include a double excess if a firm fails to take reasonable steps to verify instructions to pay or electronically transfer funds. Refer to clause 5.5 of the policy.

Watch our video

For more information on how cyber claims happen and what you can do about it watch the video of our cyber security session at this year's Risk Management Intensive available at **lplc.com.au/cyber**.

Let's improve our cyber-claims-free-days tally

To help focus on the goal of reducing the number and frequency of these claims we are going to keep track of the number of days since the last cyber notification. We will update you every week in our Friday blog.

Let's improve the current average of 19 days and start by aiming for everyone to be cyber-claim-free to the end of the year.

As at 5 September 2019

lplc.com.au/cyber