How law firms can mitigate the risk of cyber attacks

Alex Haslam is Principal of Gilchrist Connell and **Tony Reynolds** is Solicitor, Claims, at Lawcover.

Snapshot

- Cyber crime targeting lawyers is increasingly sophisticated.
- Practical steps a law firm can take to manage cyber risk include payment and instructions verification processes and staff awareness training.
- Law firms should have a plan in place for the steps to be taken if a cyber crime is attempted or effected.

Law firms hold and regularly transfer substantial funds and sensitive information, making them a target of cyber fraudsters or 'threat actors'. Over the past 12 months or so, there has been an explosion in successful social engineering and 'man-in-the-middle'-style cyber crime targeting lawyers and their clients, resulting in an increase in cyber-related claims against law firms, even when the firm's systems have not been compromised.

A change in the threat landscape

Cyber crime is now big business, costing the world over $1 trillion in 2020, and threat actors and the associated criminal enterprises that underpin cyber crime are rapidly developing their operations to make even greater profits.

Threat actors are becoming more targeted, sophisticated and efficient with their attacks. They now regularly engage in strategic reconnaissance once they have unauthorised access to a compromised system to identify the best clients and transactions to target. The timing of their involvement in transactions to redirect funds and the quality of their communications has improved. This has made their attacks more effective and more difficult to identify if proper steps and procedures to mitigate cyber risk have not been implemented.

Common scenarios and claims

The most common scenarios involve either a law firm or its client receiving a legitimate email request to transfer funds to a known or identified account. Shortly thereafter, they receive a fraudulent email that looks like it has been, or is actually, sent from the legitimate email account requesting that the transfer be made to an alternate account. Alternatively, the threat actor might set up rules to delete a legitimate transfer request and send a fraudulent request. The fraudulent email will often include a change in contact details, in addition to a change in account details, to impede attempts to verify the request. If no, or insufficient, steps are taken to verify the legitimacy of the request, the fraudulent request is then effected and the client's funds are transferred to the threat actor.

The extent to which funds transferred to a fraudster's account can be recovered is heavily dependent on how quickly the fraud is identified. In most instances, there will not be a complete recovery and the impacted client will look to the law firm to make good the shortfall. Law firms that are able to identify the procedures they have in place to prevent cyber attacks, and which have warned clients about potential cyber risks, are in a much stronger position when responding to claims.

Steps to mitigate the risk

Law firms of all sizes must take steps to protect themselves from claims arising from cyber incidents, but also to mitigate cyber risks outside of the law firm's own system.

In many instances where claims are made against law firms, there is no identifiable compromise of the law firm's systems. Instead, it is the client's system that is likely compromised, which is then leveraged by a threat actor. It follows then that the steps a law firm should take to mitigate cyber risk go beyond simply ensuring its computer systems and accounts are protected. Of particular focus should be the human factor, which is often the weakest link when it comes to cyber risk.

Law firms need to consider the risk holistically and ensure they have the following measures in place: (i) verification processes for payments and instructions; (ii) staff risk-awareness training; (iii) account, systems and network protection policies and procedures; (iv) data storage and backup procedures; (v) data security and privacy protection practices; and (vi) incident response and crisis management plans.

Policies, procedures and plans should be tested and implemented, not simply prepared as part of a tick-box exercise, given that cyber crime happens in real time and often in the maelstrom of the daily legal practice and pressures. Resources to help law firms get on top of mitigating cyber risk can be found on the Law Society and Lawcover websites. **LSJ**

The authors wish to thank Nitesh Patel, cyber expert and Special Counsel at Gilchrist Connell, for his assistance with this article.