SPECIAL FEATURE: TECHNOLOGY & THE LAW

Slack cybersecurity could bring down your law firm

Law firms are a honey pot, a place that individuals and companies will often keep their most confidential information

Arran Hunt

We'll get right to the point. Many partners are running their firms, or allowing them to be run, in a way that is detrimental to their clients. If the worst were to happen, and it is an ever-increasing hazard, partners could expect to lose any value they had in their firm as clients bail out in droves.

Cybersecurity and the risk of cyberattack still garners surprisingly little attention within the legal profession. Many firms who realise a lawyer needs to be involved seem merely to pass the issue of IT security to a junior staffer and consider it handled.

On 1 July 2021 we saw changes to the Lawyers and Conveyancers Act (Lawyers: Conduct and Client Care) Rules 2008 (RCCC). The most reported and discussed changes were those brought about by the Independent Working Group chaired by Dame Silvia Cartwright. However, other changes were also introduced. For this discussion, r10.11 expanded the old r10.4 as to the reasonable steps that needed to be taken to, in the updated wording, "ensure the security of and access to electronic systems and passwords, the protection of digital certificates and associated passwords, and the security of passwords, usernames, and personal identification numbers relating to electronic banking".

Amongst all the rules, this is the one that few lawyers would actively turn their minds to. Security seems to be something partners are willing to delegate to a third-party managed service provider (MSP). However, we would argue that such delegation is insufficient to satisfy the rules and such an approach could be detrimental to clients.

Delegation

Experts are valuable but responsibility under the rules cannot be delegated. Rule 10.11 requires the lawyer to take reasonable steps not merely to engage someone to handle security but also to ensure the job is done. Delegating a task does not meet those requirements.

The only truly secure system is one that is not used. Improper use by staff can negate any security put in place by the MSP. This could be as simple as leaving a password on a note by a PC, not having a phone properly secured or having an enabled network port in a meeting room.

MSPs are not lawyers, so are unlikely to understand all the obligations that might be required of you, whether under legislation, by the court or by clients. Firms should also not expect that of them.

Some MSPs may provide a service to a standard and in a manner that is dictated by their own preferences, or at the request of other clients. Such service levels may not be suitable to the needs of a law firm. For example, one MSP was storing a firm's files on a virtual server shared by another party. When that other party was hit by a cryptolocker, locking the files until a ransom was paid, the law firm's files were also locked as they were sharing the server. This led to the loss of a day of productivity for several dozen staff.

Treat security in a similar way to harassment or trust accounting

In another example, an MSP had a backup procedure that required manual retrieval of backups on a weekly basis. This meant files were backed up only weekly, creating a constant threat that the firm might lose a week's work had the server failed. To make matters worse, when during the 2020 lockdown no backups were taken offsite for almost two months. Any drive failure at that time would likely have ended the firm. The MSP did not make the firm aware of this failure until the country had gone to level 2.

These are just two examples of what can happen when a firm has followed the direction of an MSP or left security procedures completely in its control.

Arran Hunt

Neither situation is acceptable.

Other considerations

The preface to the rules also mentions the need to protect clients' privacy and confidentiality. This is partially covered by the correct application of r10.11. However, the Privacy Act 2020 should also be considered.

Part 6 of this Act, covered in more detail on pages 10-13, requires clients to be informed of any privacy breach that may cause serious harm. Because of the types of files firms hold for clients, almost any breach of privacy is likely to require that the client is notified. If a security breach occurs and it isn't clear if any files have been taken, you might need to notify all your clients that a breach has occurred. That would be significantly detrimental to a firm's continued operation.

Taking action

There seems to be a reluctance, especially from larger firms, to be actively involved in ensuring their systems and procedures meet these requirements. This needs to change drastically.

Law firms are a honey pot, a place that individuals and companies will often keep their most confidential information. They are the most tempting of targets, and bad actors are aware that firms are often run by people without the focus or aptitude for IT. Firms need to be more engaged in that security or risk an attack that will bring them down.

Treat security in a similar way to harassment or trust accounting. Each firm needs a security partner who can focus on ensuring r10.11 is followed. It is no less important than any other delegated role within a firm.

Arran Hunt is a partner at Stace Hammond and a member of the ADLS Technology & Law Committee

Please also see tech future, cybersecurity and comp law