Data Security – What next?

Once you have answered some key questions regarding data and cyber security at your law practice, it's time to look at implementing appropriate levels of protection.

Classify your data

Having established the various types of information held by your law practice online, you can consider what protections you need. Information classifications may assist in considering the appropriate level of protection.

For example:

Restricted: The most sensitive data that could cause great harm if compromised. Access is strictly limited.

Confidential or Personal: Sensitive data which, if compromised, could give rise to reputational, regulatory or commercial harm to the law practice, it's client or other third party. Access is restricted to the company or department that owns the data, on a 'need to know' basis.

Public: Non-sensitive data that would cause little or no risk to the practice if accessed. Access is loosely, or not at all, controlled.

After classifying your data, create a strategy to protect each level appropriately. Review who has access to the various levels and the technical controls in place. Talk to your IT provider for their insights into security and educate staff about their role in keeping information safe.

Access

Once you have identified all those with the potential to access your data, review their levels of access and decide who should access certain files, databases, mailboxes, calendars etc. Limit access given to external providers and restrict access to accounts such as supplier websites and social media. Remember to revoke access to systems and data when an employee changes roles or leaves the law practice. Keep records and document procedures.

> If you believe you have been subject to a cyber breach or attack, take steps immediately to ensure your systems have not been compromised. Contact your IT consultant or the Lawcover group cyber risk policy crisis management team on **1800 BREACH (1800 273 224)**.

Give staff the minimum permissions they need to perform their work to reduce the risk of an 'insider' accidentally or maliciously endangering your practice. You can always change access levels or permissions as required.

Practice procedure and policy

Do your documented policies match what is actually happening in practice?

All too often, written policies and procedures can become a 'tick box' form of compliance made worse when the information in these documents don't line up with what is actually happening in the practice.

Consider whether your policy or procedure is accessible, easy to read and addresses all the threats and risks that the practice faces. Ensure staff are trained in procedures and are regularly updated on policy changes and requirements.

Stay informed

Ensure staff are trained in recognising cyber threats, remain informed of emerging threats and know what to do in the event of a cyber breach. Lawcover has a number of useful cyber resources that detail the types of threats law practices face and the steps you can take to protect your practice. Lawcover also provides a complimentary eLearning course on "Cyber claims in legal practice" which contains useful examples of the types of attacks experienced by law practices and what you can do to manage the risk. This course is available on the Risk Online eLearning platform - Register for the course. The Australian Cyber Security Centre also provides a cyber alert email service you can sign up for to receive regular updates on general cyber security trends and emerging threats.

Candice Perriman
Rick Education Manager