Why cyber security is not the same as IT support

Cyber attacks pose a serious risk to data and system security, client relationships and confidentiality, and law practice resilience and reputation. This is why law practices must adopt proper cyber risk management and not assume that your internal or external IT support provider has it covered.

Ask yourself these questions about your cybersecurity.

Who is currently undertaking and documenting your cybersecurity vulnerability risk assessment?

Vulnerability risk assessments are an essential first step towards cyber security. Assessments should be undertaken periodically by someone with cyber risk management experience, and they should know the current methods of entry and forms of attack (such as impersonation fraud, ransomware, phishing scams etc). An assessment should include scanning and probing for vulnerabilities in systems, technology and hardware and current configurations should be reviewed.

In addition, assess the risks associated with staff and the way they use technology and systems of work, as well as interactions with clients and the platforms the practice relies on (e.g. electronic banking).

Who is configuring your security?

While essential to the daily operations of a law practice, IT support serves a different purpose. Using the results of the vulnerability assessment, a cybersecurity professional can determine how to configure your technology appropriately. It is important that configuration provides protection against attacks without interfering with daily functionality. Firewalls, anti virus software, logins and access permissions, personal devices, remote connections, back ups, user privileges, logs, and detection alerts are just part of a long list of areas requiring attention.

Who is providing cybersecurity awareness training and education to staff?

Making staff aware of the type of dangers that exist, including the tricks being used to gain access to confidential information, your systems and data is key to preventing a cyber security incident. Test that the training is working, by simulating attacks and use the results to inform further training.

Do you have the right policies and procedures in place?

Your systems are most secure when people know how to use them safely. Defining and communicating policies and procedures will help prevent and manage security incidents. Make sure staff are trained and informed so that everyone knows what is expected of them.

Are you investing in the right security software?

Security software is not a one size fits all solution. Different programs do different things and investing in additional software may not always solve your security problems. In fact, sometimes this can make things worse. Make sure your security software is working for you and not against you. Check you have the right measures in place that address key areas of vulnerability and that these measures are switched on and configured correctly.

Who is providing you with ongoing assurance that your security controls remain appropriate and effective?

IT support are not cyber security experts and assurance is not a one-off spot check. Over time technology changes, threats and forms of attack become more sophisticated. Testing and auditing your cyber security controls should occur on a regular basis to ensure you have continued protection and systems remain up to date.

Don't assume your IT support has your cyber security needs covered. Use the right people for the right job and take the necessary steps to ensure your practice has a strong defence.

Candice Perriman
Risk Education Manager