Top tips for minimising cyber attacks

Cyber security has never been more important, particularly for a legal practice.

Implementing the following risk management tips will not only set you on the right path to minimising your exposure to a cyber attack, it will also ensure that regular updates and evaluations take place to minimise ongoing risks.

Tip 1 - Confirm account details over the phone before processing funds transfers

The most frequent form of cyber-attack against legal practices are Business Email Compromise frauds (BEC). BEC frauds occur when a cybercriminal impersonates a client, vendor or employee of the practice and issues fraudulent instructions to initiate the transfer of funds or sensitive information.

These attacks frequently occur in conveyancing matters, typically as a result of a security breach of the company's computer network (or that of a Third Party) from phishing attacks, email spoofing or through social engineering.

Whilst these attacks can be sophisticated, BEC frauds rely on an individual (e.g. employee) to execute the funds transfer.

Examples of 'red flags' associated with BEC frauds include:

- The sender purports to be someone in a position of authority (e.g. CEO, CFO, partner)
- Emails requesting urgent payment or threatening consequences if payment isn't made
- A vendor has provided new bank details
- The sender requests payment of an invoice outside of the usual payment cycle.

To limit the risk of BEC fraud, ensure that any transfer details have been confirmed with the issuer over the phone. It is important to use existing contact details. Never use contact details from a suspicious email. In most instances, a simple call to the issuer will provide clear confirmation of all details.

If the issuer has no record of the email requesting the transfer then treat the email as suspicious, contact your IT consultants and notify Lawcover of the incident by calling 1800 BREACH immediately.

Tip 2 – Implement multi factor authentication (MFA)

Multi factor authentication (MFA) requires more than one form of authentication to verify a user's identity before allowing them to login or perform certain types of transactions.

MFA creates a layered defence system which greatly reduces the likelihood of cybercriminals successfully hacking your legal practice network.

MFA can be incorporated into most business programs and is an existing feature on systems like Office 365. If MFA is not enabled on your computer network, contact your IT consultants and enquire about installing.

Tip 3 - Ensure regular software updates and patching

Regardless of size, every legal practice should ensure that optimal business security and anti-virus protection software is installed on each device within their network.

However, keep in mind that while installing security software is important, maintaining it is essential to keep it working effectively. Cybercriminals can detect and exploit security holes or software vulnerabilities that may exist in ageing systems.

Regular updates and patching are essential to guarantee that security flaws are removed and ensure the ongoing effectiveness of your IT security systems.

Tip 4 - Conduct regular cyber security audits, including penetration testing

In addition to regular software updates and patching, it is important to conduct regular security audits to identify potential weaknesses in the existing IT security systems.

Security audits often involve a series of tests including:

- Penetration testing - simulations of attacks that may be employed by hackers
- Awareness testing - simulated phishing scams or social engineering techniques to ensure staff are aware of, and following, existing protocols
- Security review - identify and test existing security software to ensure effectiveness
- Ensure that back-up systems and protocols are functioning effectively - this is important to minimise the risk of ransomware attacks and subsequent business interruption.

IT consultants can conduct audits to accurately test the strength of existing systems in your legal practice.

Tip 5 - Formulate a cyber incident and privacy breach response plan

A serious cyber incident will likely catch you off guard and result in confusion, delays and mistakes which worsen the impact of the incident.

To ensure you are able to manage a cyber incident effectively, prepare a cyber incident response plan and privacy breach response plan which can be accessed by all employees.

Any cyber incident or privacy breach response plan should include notification to Lawcover via 1800 BREACH and should clearly outline the immediate steps to be taken in response to a cyber incident, including:

- Appointment of IT consultants to assess the extent of the incident
- Identification of important data and critical systems
- Key roles and responsibilities, including internal notification protocols
- Stakeholder communication protocols (public relations and media management)
- Reporting obligations (particularly under the Privacy Act 1988).

Remember, a cyber incident may result in the complete shutdown of your computer network so ensure hard copies of each plan are available to all staff.

Cyber attack is a real threat to legal practice and could result in significant business, revenue and reputational loss. However, anyone with basic computer knowledge can take fundamental steps to keep their network and data secure from cyber attack. Following these key tips is a great way to start.

Lawcover is pleased to offer "Cyber claims in legal practice"- a complimentary course available on our Risk Online eLearning platform. Click here to register for the course.