COLIN BIGGERS & PAISLEY LAWYERS

Top 5 tips to minimise the risk of cyber-attacks

1. Confirm account details over the phone before processing funds transfers

The most frequent form of cyber-attacks perpetrated against Law Practices are Business Email Compromise (**BEC**) frauds. BEC frauds are an online scam where a cybercriminal impersonates a client, vendor or employee of the Law Practice and issues fraudulent transfer instructions to induce the transfer of funds or sensitive information.

This issue is particularly prevalent in conveyancing matters or other instances where the company does not regularly transfer funds with the Third Party.

These attacks usually occur as a result of a security breach of the company's computer network (or that of a Third Party) as a result of phishing attacks, email spoofing or through social engineering techniques.

Whilst these attacks can be sophisticated, BEC frauds still rely on an employee or agent of the company to execute the funds transfer. Therefore it is important that employees are aware of the 'red flags' that may indicate a BEC fraud:

- The sender purports to be a someone in a position of authority, particularly if such a person wouldn't normally issue payment requests
- Email requests urgent payment or threatens 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 or the invoice amount is larger than usual

Another simple measure businesses can take to limit the risk of a BEC fraud is to ensure that the transfer details have been confirmed over the phone with the issuer. It is important to use contact details not contained in the suspicious email, but rather use existing contact details.

In most instances a simple call to the issuer will confirm that they have requested the payment and that the account details are correct. If the issuer has no record of the email requesting the transfer treat the email as suspicious and contact your IT consultants and cyber insurers immediately.

2. Ensure multi factor authentication (MFA) is enabled

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

Whilst cybercriminals can employ a variety of techniques to attempt to access the Practice's computer network (phishing, malware, social engineering, brute force attacks) MFA creates a layered defence system which greatly reduces the likelihood of cybercriminals successfully hacking the network.

MFA can be incorporated into most essential business programs and is an existing feature on systems like Office 365. If MFA is not enabled on your computer network we encourage you to contact your IT security provider.

3. Ensure regular software updates and patching occurs

All businesses, regardless of size, should ensure that optimal business security and anti-virus protection software is installed on each device within the company's computer network.

Whilst installing security software is important, cybercriminals can detect and exploit security holes or software vulnerabilities that may exist in ageing systems. Such security flaws can leave the computer network exposed to malware or other forms of attack.

Regular software updates and patching is important to guarantee that security flaws are removed, ensuring the ongoing effectiveness your IT security systems.

4. Conduct an annual cyber security audit, including penetration testing

In addition to ensuring regular software updates and patching, it is important that the company engages in annual security audits to identify potential weaknesses in the existing IT security systems.

Security audits will involve a series of tests including:

- Penetration testing. Simulations of attacks that would be hackers could employ.
- Awareness testing. Simulated phishing scams or social engineering techniques to ensure staff are following existing protocols
- Security review. Identify and test existing security software to assess adequacy.
- Ensure that back-up systems and protocols are functioning effectively. This is important to minimise the risk of ransomware attacks and subsequent business interruption.

Whilst security audits can be handled internally, best practice is to have external IT consultants conduct the audit to accurately test the strength of existing systems.

5. Formulate a cyber incident and privacy breach response plan

In many instances a serious cyber incident will catch a company unawares, resulting in confusion and delays which can worsen the impact of the incident.

In order 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 response plan or privacy breach response plan should include notification to your cyber insurer via the 1800 BREACH hotline.

In addition, the plan should clearly outline the immediate steps which should 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*)

As a cyber incident may result in the complete shutdown of your computer network, ensure hard copies of the relevant plans are available in each office.