Cyber Safe Or Cyber Sorry?

Risk Management Topic:

Cyber Security

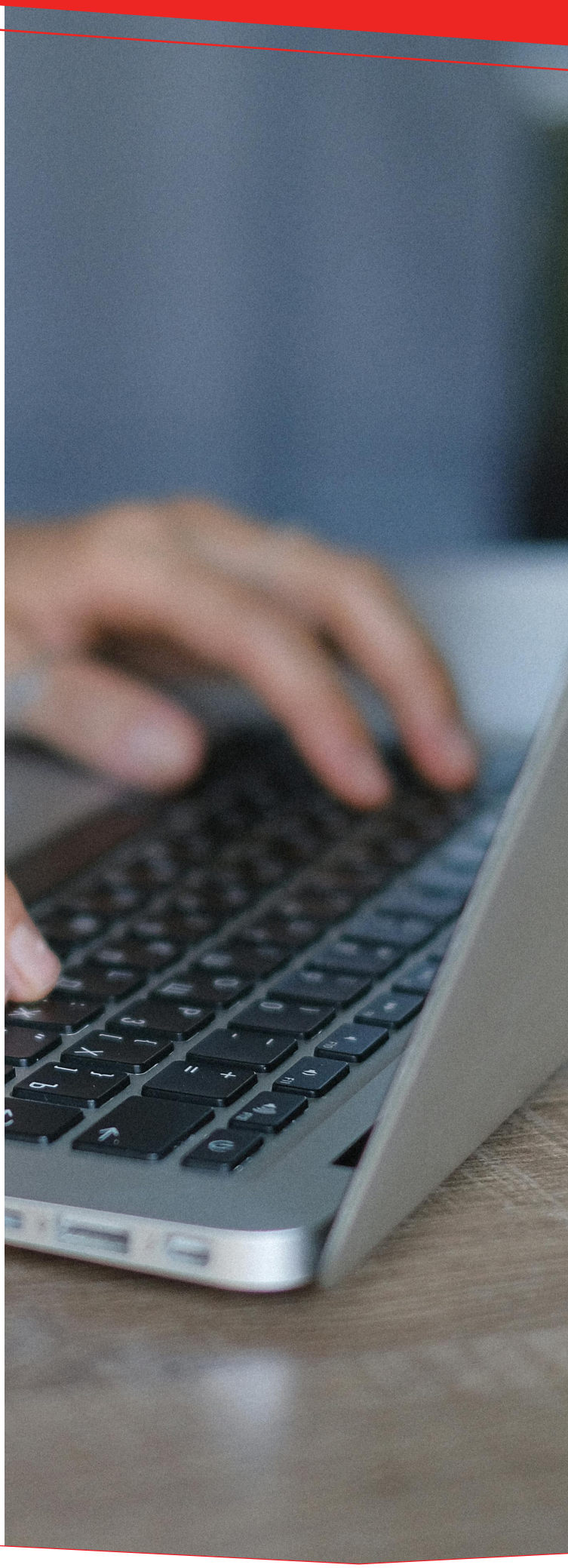
Mili Vukancic
Claims Team Leader

Cyber criminals aren't just tech savvy, they're transaction savvy too. They know how legal practices operate, and they're using that knowledge to strike at the most opportune moments.

Lawcover continues to see claims involving cyber assisted fraud, especially payment redirection scams.

These often happen during property transactions, when timing is critical and trust accounts are being used. A compromised email (known as Business Email Compromise) can lead to a fake request to change bank details, and suddenly, your client's funds are gone. The client may be in breach of contract, and your practice is left scrambling to recover the money and reputation.

What's alarming is how well these criminals understand legal workflows. They know when large transactions and settlements occur, how trust accounts are structured, and how to convincingly impersonate legitimate communications between solicitors, clients, and financial institutions. This isn't just a cyber security issue; it's a professional and operational risk.



Cyber Safe Or Cyber Sorry?

What can you do?

- Add your trust account details to your Costs Agreement and tell clients those details will never change by email

- Before transferring funds, verify account details by phone:
  - Make an outbound call using a known phone number (not a number provided in an email) to check the account details
  - Be sure to verify the person you are speaking with
  - Check the account details
  - Remind your clients and other payers to do the same

- Add multi-factor authentication as an additional layer of security

- Conduct regular audits and security penetration testing to ensure your practice systems are up to date

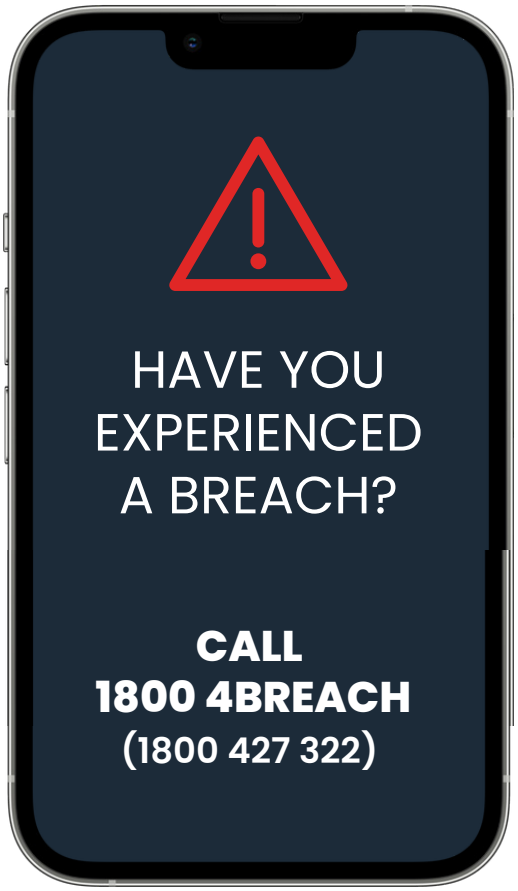
- Work with reputable cyber security experts to ensure vulnerabilities are addressed and robust security measures are in place and maintained

- Training. Cyber security isn't just for IT, it's for everyone. Make sure your team knows how to spot suspicious emails, verify payment instructions, and respond quickly to incidents

Cyber Safe Or Cyber Sorry?

If you suspect your system has been compromised:

- Contact your IT service provider and advise them of your suspicions
- Contact Lawcover's Group Cyber Policy Response Team on **1800 4BREACH (1800 427 322)**
- Notify relevant government agencies like the Australian Cyber Security Centre and Scamwatch. Even if no money is lost, report the incident. Every alert helps build a stronger defence



Cyber Safe Or Cyber Sorry?

If money has gone missing?

- Immediately notify your bank's fraud team

- Contact Lawcover's Group Cyber Policy Response Team on **1800 4BREACH (1800 427 322)**

- If trust money is involved, contact the Law Society of NSW's Trust Accounts Department on **(02) 9926 0337**

- Contact the affected client and advise them to urgently notify their bank to intercept the transaction or assist in recovering the funds

- Undertake an immediate audit of your files and contact all clients with upcoming settlements or other payments

- Warn clients not to rely on email requests for the transfer of funds without first confirming the instructions, preferably in person, or at least by phone, using a verified contact phone number

- Conduct an audit of recent transactions to make sure that an earlier fraudulent interception of funds has not occurred

Cyber fraud is always evolving, which means your defences must also evolve. Ensure you have the right support, systems, defences and procedures in place and stay informed and protected.

For comprehensive guides and resources on cyber security that are tailored for legal practices see below.

Click here for more information >