SIMON COHEN *Founder / Owner & CIO Cohesis Pty Ltd*
www.linkedin.com/in/simoncohen1/
www.cohesis.com.au

"Helping businesses implement IT strategies to drive growth, reduce Cyber risk and increase operational effectiveness."

TIP 1: CYBER AWARENESS TRAINING

Business leaders often 'forget' that employees are the first line of any organisation's Cyber defence. Cohesis recommends that ongoing Cyber Awareness training and testing is conducted.

TIP 2: FIX POOR USER BEHAVIOUR

Weak passwords, poor browsing habits and a "do it later" attitude to installing updates, all weaken an organisation's Cyber posture. Strong governance and effective communication are vital to fixing poor user behaviour which can otherwise lead to vulnerabilities in corporate networks.

TIP 3: BE PREPARED - ASSUME YOU WILL BE A VICTIM OF A CYBER ATTACK

The likelihood is that your organisation will suffer a Cyber Attack. Being prepared and having a plan helps you take control of the situation which will build trust with your staff, customers and stakeholders. Cohesis recommends organisations to develop a Cyber Incident Response Procedure.

TIP 4: SENIOR MANAGEMENT NEED TO COLLECTIVELY 'OWN' THE CYBER SECURITY AGENDA

It's important for leadership teams to collectively 'own' the Cyber Security agenda. Organisations that struggle to implement effective cyber security measures, do so because of a belief that 'Cyber' is purely an IT problem and fail to obtain 'buy-in' and support from other senior managers and functional areas.

TIP 5: CYBER SECURITY IS A PROCESS, NOT AN EVENT

Effective Cyber Security should be viewed as an ongoing process. A single penetration test, policy or training video is insufficient to meet the evolving threat landscape. Organisations need to implement a process of continuous improvement focused on identifying and managing risks before they can become issues.

TIP 6: IMPROVE LEVELS OF IT GOVERNANCE AND COMMUNICATIONS

IT governance is frequently perceived as dull and bureaucratic, but it can mean the difference between business success and failure. Cohesis recommends to engage an expert who can help you create effective cyber security policies and procedures.

TIP 7: TEST YOUR ABILITY TO RECOVER

If your software is hosted 'on premise,' make sure that your IT support provider tests your backups and can prove that, in the event of a Cyber Incident, they can effectively recover your systems and data.

TIP 8: DON'T ASSUME THE 'CLOUD' WILL PROTECT YOU FROM A CYBER ATTACK

There is a common misconception amongst many business leaders that moving to the cloud provides a shield against all cyber attacks. While cloud vendors take security (and the marketing of their Cyber credentials) very seriously, no system or service is ever 100% secure.

TIP 9: ENSURE YOUR SYSTEMS AND DATA ARE RESTRICTED TO A 'NEED TO KNOW' BASIS

Ensuring access to networks, systems and data is provided on a 'Need to know' basis reduces the probability of 'insider' data leakage and data breaches.

TIP 10: MOBILE DEVICE MANAGEMENT

Organisations that allow corporate data to be accessed from mobile devices should employ effective Mobile Device Management - aligning technical capability and company policy to ensure staff accept that compromised devices may be locked or wiped.