KAREN STEPHENS

Karen is CEO and co-founder of BCyber, an agile, innovative group that works with SMEs to protect and grow their businesses by demystifying the technical and helping them to identify and address cybersecurity and governance risks. In 2021 Karen graduated from the Tech Ready Woman Academy's Accelerator and the Cyber Leadership Institute's CLP programs.

COLUMN

Keep calm and carry on

As I sit down to write this Australians find themselves knee deep in the Optus data breach.

It is all very good to say "keep calm and carry on" but the 9.8 million Australians who may have been affected (and some say the figure could be as high as 11 million) is a substantial portion of our population, which stands at around 25 million. So, I fear this message is perhaps not getting through to those who need it the most.

As always it is important to have good cyber hygiene at both a personal and a corporate level. So, while the mainstream media keeps on feeding the fire of fear and confusion, we need to keep our heads when all about us are losing theirs (with thanks to Mr Kipling) and focus on ensuring we get the basics right. Here are six basics to get you started on the cyber secure journey.

1. **Assessment.** You cannot protect what you are not aware of. You cannot educate those you do not understand. A good assessment includes both qualitative and technical quantitative components. And do not forget to include your website!

2. **Good password hygiene.** We saw how important this was during the recent RI Advice court case. While it may be tempting to use a password more than once, to share it (to keep software costs down) or even to choose one you can easily remember, don't. You need passphrases or a complex password containing 16 alphabetic and non-alphabetic characters for everything: business, personal, the lot.

3. **Build cyber knowledge into your DNA.** Tick-the-box cyber training leads to complacency and a false sense of security. Training and education must be continuous, relevant and fun.

4. **Patch everything, patch often, patch now.** Do not make it easy for cybercriminals to exploit your business. Keep your patches up to date on all devices; business and personal.

5. **Speak business not tech.** Never assume your business contacts understand what you are saying. There are many interchangeable terms out there. ATO, is it Australian Tax Office or Account Takeover? Assets, do you want to invest in shares, property, fixed interest accounts or cash, or do you mean software and hardware? There are many more examples, but you get the gist.

6. **Practice makes perfect.** When you have a ransomware breach, that is not the time to discuss how to handle it. The better prepared you are, the better your business will handle the breach.

www.linkedin.com/in/karen-stephens-bcyber

www.bcyber.com.au

karen@bcyber.com.au

twitter.com/bcyber2

youtube.bcyber.com.au/2mux