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

Don't get poor fast!

With Australia still suffering from a number of significant data breaches (you know who they are) we have a lot of negativity. So, rather than end the year on a note of doom and gloom, I thought I should take a retrospective look at these breaches. There are three things we can learn: the silver linings in rather dark and stormy clouds, so to speak. These could save you time, money and (in some cases) your business.

Cyber awareness is key. Change the narrative from "your staff are your weakest link" to "your staff are your first and best line of defence." So, no more "speaking at them," trying to bore them into submission. No more once-a-year conferences and training workshops that focus on the 'magic' of a breach with live demos of mobile phone hacks (rather than on what to do to stop them). No more of the same boring awareness training year after year. ***Make 2023 the year you change it up. Make your cyber awareness training interesting, practical, relatable and memorable.***

Do not forget your client. While cyber awareness improvements across your organisation—from the mailroom to the boardroom—are key to your business' cyber safety, what about taking your clients on the journey? In 2023 strengthen your client relationships by helping them build their cyber resilience. Simply add cybersecurity to your onboarding process, annual reviews or even your newsletters and/or email communications. Many clients may not understand phishing scams, the issues that arise from using personal email accounts to store company data, the importance of good password hygiene or staying up-to-date on the latest data breaches. ***Making sure your clients are more cyber-aware could be the best five minutes you spend with them.***

Good password hygiene is for everyone and forever. Password hygiene might not be exciting, but it sure does pack a powerful punch. Make 2023 the year you review your current password policies. Provide them in writing to all staff, check in to see they are being followed and encourage their use in employees' personal lives. ***Good password practices are for everyone and should not stop when they leave the office, are at home and/or have stopped working.***

You may be thinking "This is all very well and good, but what has this got to do with "don't get poor fast?" Well, by implementing these three recommendations – you might just avoid a cyber breach and then you will not need to pay:

- Cyber breach costs: the average cost of a breach was $2.92m in Australia in 2022.
- Data breach penalties: the Australian government is to the greater of $50m, three times the value of any benefit obtained through the misuse of information, or 30 percent of a company's adjusted turnover during the breach period.
- More data breach penalties: under the National Data Breaches scheme, failing to report a breach can cost from $444,000 for individuals to $2.2 million for companies.
- Director penalties: these can cost up to $200,000 for a breach of s180 of the Corporations Act 2001.

There are other costs that can result from a data breach, but because we are trying to end the year on a positive note, I shall assume you get the general idea. The takeaway is this:

It is cheaper to take action to prevent a cyber breach than it is to wade through one and remediate it!

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

www.bcyber.com.au

karen@bcyber.com.au

twitter.com/bcyber2

youtube.bcyber.com.au/2mux