KAREN STEPHENS

Karen Stephens is the co-founder and CEO of BCyber. After more than 25 years in financial services, Karen moved into SME cybersecurity risk management. She works with SMEs to protect and grow their businesses by demystifying the technical aspects of cybersecurity and helping them to identify and address cybersecurity and governance risk gaps. She was recently named inaugural Female Cyber Leader of the Year at the 2023 CyberSecurity Connect Awards in Canberra.

COLUMN

Who should be in security?

Who should be in security? That's a big question with a simple answer. And the answer is… absolutely everyone!

2024 started with the proverbial Big Bang. We had the mother of all breaches with 26 billion records leaked from multiple sites, including Tencent, Weibo, Twitter, LinkedIn, Adobe and Canva; a mind blowing 12 terabytes of data. It is difficult to comprehend such massive data volumes. This will provide some perspective: Many ISPs cap monthly data usage at one terabyte[(1)] the Hubble Space Telescope generates about 10 terabytes of new data every year[(1)] and IBM's famous Watson game-playing supercomputer has 16 terabytes of RAM[(1)]. So it was a mega leak, and it may not include recent Australian based breaches like Nissan Australia, the Victorian courts or The Iconic.

If you are thinking, "well so what?", these breaches have given cybercriminals access to a huge database of personal information that can be used for credential stuffing activities, where cybercriminals use the leaked customer credentials to try to log into other websites. Some will be successful because many people reuse login credentials for more than one website. It was this type of breach that saw customers of The Iconic flood its Facebook page with complaints of fraudulent orders placed in their names.

So, in my opinion, we are now all casualties of the data privacy wars. No one is left untouched, and security is now the responsibility of us all. Cybercriminals do not respect age, gender, or geographical boundaries. If you are connected to the Internet, you are fair game. And the risks are unavoidable unless you are living totally off the grid with no Internet. Nor can cybersecurity give you 100 percent foolproof protection, 100 percent of the time. Good cybersecurity means acknowledging the risks and getting the basics right, all the time.

It is all well and good to say we all need to harden our cyber resilience to be more cyber safe, but sometimes even getting started is the most confusing and challenging part. Looking beyond security software and all it entails, here are four steps to get you (and your family) started:

Good password hygiene. Passwords are an important line of defence when it comes to protecting your data. Increase your personal cyber resilience by:

1. Keeping your passwords safe. Do not write them on sticky notes, reuse them or share them.
2. Choose complex passwords. Have at least 16 random characters.
3. Keep an eye out for news of major breaches/ leaks and update your passwords if you think you have been caught up in one.
4. Never use any personal details in your passwords.

Responsible social media use. Social media is a great source of useful information for cybercriminals. Be aware of what you share online, not only about yourself but about your family and friends. Remember everything you share on social media can and will be used against you. A quick preventative measure is to lie (yes lie) when completing security questions, just in case you have overshared personal information on a social media account.

Cyber awareness training. This is not needed only by workers. Everyone, young and old, need to have some cybersecurity training. There are many free online training programs available where the only cost