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

Rising phoenix a tale of resilience and renewal

Don't we all wish we had a phoenix, like the one in the Harry Potter books. Because, like Harry Potter, we sometimes need someone to swoop in and save us. Sadly, there are no such magic fixes. And, if I have learnt anything since moving into cybersecurity, it is that you need to build your own fortress to save yourself.

Regular readers may remember that, after spending more than two decades in the financial services industry at some of Australia's largest firms, I transitioned into cybersecurity risk management, where I find I am often the phoenix for others: those entertaining the idea of moving into cybersecurity and/or startups and who want to bake-in cybersecurity from the get-go.

What would your personal phoenix say to a newly minted cybersecurity risk management person?

- **Skills audit.** The skills acquired in your business or university life can be easily transferred to new industries. In my case the exciting world of cybersecurity was the industry calling my name. The ability to talk to people and make the highly technical language of cyber palatable and understandable for clients is a much needed and rather rare skill set. Tech can be taught. Client service skills are much, much harder if not nigh on impossible to teach.
- **Cyber is not just tech.** Yes, there are lots of highly technical roles. We are all familiar with 'sexy' threat hunter roles (please refer to almost

any movie referencing cyber), but cybersecurity should not be about tech alone, it should be about the transference of knowledge. Within a business those holding the proverbial cheque book are not usually the heads of technology. Their ranks are more likely to include the CEO or head of risk: people who find themselves having to meet regulatory and legislative responsibilities that can have significant downsides if unmet. These are the key staff who need to understand that cybersecurity is a business risk with an immense downside if ignored or glossed over.

- **Be a translator.** A sad but true fact is that technical jargon does not always carry over seamlessly between industries. For example, in cybersecurity ATO stands for Account Take Over and in financial services for the Australian Taxation Office. Both can strike fear into the hearts of a business, but for different reasons. So make sure you know your client's language as well as you do your cybersecurity language, and when in doubt spell it out!
- **It takes a village.** Finding community support was vital during my transition into cybersecurity risk management. I engaged mentors and joined groups like AWSN whose members have been incredibly generous with their time and insights. The challenge lies in seeking assistance when needed.

As I find myself settling into this amazing industry I want to pay it forward, and that is why I am always up for a cybersecurity coffee chat and for (trying) to be a personal phoenix where I can.

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

www.bcyber.com.au

x.com/bcyber2

karen@bcyber.com.au

youtube.bcyber.com.au/2mux