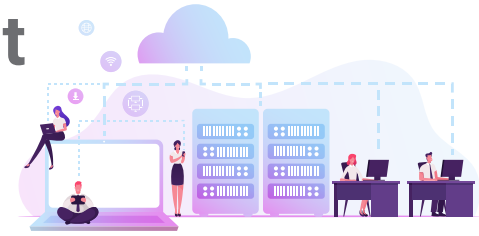
KAREN STEPHENS

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

Cybersecurity is not just about technology



Cybersecurity is much more than a technology problem with only technology as its solution. We need to look at cybersecurity through a broader lens without getting bogged down in the technical aspects and ignoring the, critical, people component.

Taking a human-centred approach to cybersecurity means emphasising the importance of all staff and their roles in ensuring cyber threats are mitigated. As someone (relatively) new to the cybersecurity industry, it is my view EVERYONE in the business plays a part in hardening cyber resilience.

A strong human line of cyber defence is a crucial element of a successful cybersecurity strategy, and one which can often be overlooked. In this human line of defence, diversity is Queen (or King). Imagine how much stronger your cyber resilience programs would be if:

- Your cyber awareness education program was regular, relevant and practical across the entire business, with everyone from the boardroom to the mailroom taking an active part. Think of this as building a reinforced brick wall to secure your entire business from external cyber threats. This would be a far better approach than having only some areas secure, which is what you get when you have an ad hoc, poorly-delivered program (i.e., a brick wall with holes).
- Cybersecurity was baked into every project from the 'get-go'. For example, if HR wants to implement a new system, you make sure the steering committee has someone involved who understands cybersecurity and can provide a cybersecurity viewpoint.
- Each department had its own internal cybersecurity champion, creating a two-way information sharing opportunity. If the non-IT rep can understand and communicate what IT is trying to implement, they would be able to spread cyber resilience throughout the business. As a bonus you may even attract staff who would never have thought of cybersecurity as a career but whose life skills can round out your IT team beautifully. Tech skills can be taught, life skills not so much!
- Tech project teams included non-tech stakeholders as a business-as-usual activity. This is particularly helpful if you need to present to and get signoff from your executive leadership team and/or board. The addition of these stakeholders will help you understand business drivers and values, allow you to deliver a plain English version of what may well be a highly technical project presentation, and increase the likelihood of your business case getting approved.

Using diversity of knowledge and experiences within a business to harden cyber resilience. That is priceless.

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

www.bcyber.com.au

karen@bcyber.com.au

twitter.com/bcyber2

youtube.bcyber.com.au/2mux