KAREN STEPHENS

Karen is CEO and co-founder of BCyber, an agile, innovative group who works with SMEs to protect and grow their business, by demystifying the technical and helping them to identify and address cybersecurity and governance risk gaps. Karen has recently graduated from both the TechReady Woman Accelerator graduate and CLP program with the Cyber Leadership Institute in 2021.

COLUMN

Don't ask who runs cyber. Ask who should run cyber

The way we work has changed thanks to the pandemic. We are now all doing some variation of the work from home/work from the office two-step. So, it makes sense to rethink how we view cybersecurity: its ownership and responsibilities.

So "who runs cyber?" is not the real question, it's more a question of "who should be running cyber?" The answer is: a business/IT hybrid team - the ultimate symbiotic relationship.

Want to know why?

The lines between IT and business are becoming increasingly blurred as SMB owners become the default "inhouse technical experts"

Recent statistics have small businesses and family enterprises representing 97% of businesses in Australia. Traditionally, they are left behind when it comes to cyber security. They are considered too small by the big consultants or are unable to afford the measures and staff available to big businesses. This means they often end up with a mish-mash of cyber security measures made up of 'do-it-yourself' plus 'outsource some' plus 'what free stuff I can find to make do with?' There is no clear coordinated strategy. As a result, the delineation between technical and business becomes blurred.

There are no blank cheques

Securing an entire business is an unrealistic goal but it is the business and not IT (the IT department in a big business or the external service provider to a small business) that makes the ultimate decision around spending, delicately balancing "How much risk is the business willing to accept?" versus "How much security can the business afford?" It is IT that provides each business with the ability to make the most appropriate decision.

Silos are so old school

Cyber security cuts across every department and through every level of an SMB. Hoping to "keep the cybercriminals out" is not the sole responsibility of IT. Everyone in a business — whether it be large or small — needs to be cyber aware because everybody has something of value. For example, HR is responsible for personally identifiable information; Finance for client invoicing details; Compliance for all corporate activities; Operations for insurance policy terms and conditions, etc. In an SMB all those business units may be just one or two individuals. A single machine or server going down can mean the loss overnight of a business that has taken years to build.

A business, its IT and its cyber security need to be in lock step. No cyber security can mean no business.

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

www.bcyber.com.au

karen@bcyber.com.au

twitter.com/bcyber2

youtube.bcyber.com.au/2mux