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

Improving security together

Another month and another gentle (or maybe not so gentle) push from the government to get our cybersecurity house in order. Since 8 July we have been working under the newly amended Security of Critical Infrastructure Act 2018 (SOCI) Act.

This is a great opportunity to move our cybersecurity discussions from the "it's a technology problem" silo into the "let's embed cybersecurity into the broader business risk program" to imagine working as one team to improve our cybersecurity.

Here are a few points to get the conversation started.

DO YOU KNOW IF YOUR BUSINESS HAS NOW BEEN 'CAPTURED' BY THE SOCI ACT?

The definition of what constitutes critical infrastructure has been expanded. The SOCI Act now places obligations on specific entities in the electricity, communications, data storage or processing, financial services and markets, water, healthcare and medical, higher education and research, food and grocery, transport, space technology, and defence sectors.

HAVE YOUR BUSINESS PROCESSES AND PROCEDURES ACROSS ALL DEPARTMENTS BEEN UPDATED TO ENSURE REPORTING OBLIGATIONS CAN BE MET?

Your reforms need to be addressed holistically rather than with the traditional siloed approach. Cybersecurity cuts across all departments: finance, people and culture, sales, marketing, etc.

DOES YOUR BUSINESS KNOW WHERE TO START?

As businesses look to incorporating changes to their risk management programs, a logical place to start may be IT asset management with the key asset register serving as a single source of truth accessible through a single secure portal.

DOES YOUR BUSINESS KNOW AND UNDERSTAND THE REPORTING TRIGGERS AND REQUIREMENTS?

There will be some slight variations depending upon 'criticality' and 'sector', but, under the SOCI Act's requirements for cybersecurity incident reporting:

- "If you become aware that a critical cybersecurity incident has occurred, or is occurring, AND the incident has had, or is having, **'a significant impact'** on the availability of your asset, you must notify the Australian Cyber Security Centre (ACSC) within **12 hours** after you become aware of the incident. If you make the report verbally, you must make a written record through the ACSC's website within **84 hours** of verbally notifying the ACSC."
- "If you become aware that a cybersecurity incident has occurred, or is occurring, AND the incident has had, is having, or is likely to have, a **'relevant impact'** on your asset you must notify the ACSC within **72 hours** after you become aware of the incident. If you make the report verbally, you must make a written record through the ACSC's website within **48 hours** of verbally notifying the ACSC."

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

www.bcyber.com.au

karen@bcyber.com.au

twitter.com/bcyber2

youtube.bcyber.com.au/2mux