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

Progress not perfection might just be the key

There are many people making a difference in cyber security and how it is viewed by our clients, but I would like to draw attention to a Federal Court ruling in May of this year when, for the very first time, an Australian Financial Services Licensee (AFSL) was found to have failed to adequately manage its cyber security risks (the ruling).

The message that cyber security should be top of mind for all businesses (especially those in the advice space) was clearly spelt out by her honour Justice Rofe when she stated "Cyber security risk forms a significant risk connected with the conduct of the business and provision of financial services. It is not possible to reduce the cyber security risk to zero, but it is possible to materially reduce cyber security risk through adequate cyber security documentation and controls to an acceptable level."

This translates to: while nothing is 100 per cent perfect, progress and not perfection is key.

The cyber security pathway for AFSLs is now clearer with the Australian Securities and Investments Commission (ASIC) advising they:

"Should be aware of the potential consumer harms that arise from cyber security shortcomings."

"Should adopt good cyber security risk management practices to reduce potential harm to consumers. … [Practice] active management of cyber risks and continuous cyber security improvement, including assessment of cyber incident preparedness and review of incident response and business continuity plans."

are expected "to act quickly in the event of a cyber incident to minimise the risk of ongoing harm … [and all] … should regularly reassess their cyber risks and ensure their detection, mitigation and

response measures adequately support the size and complexity of their business and the sensitivity of the information they hold."

Three key responses are needed:

Cyber education should be a key foundation of risk mitigation programs. They should be ongoing and not a one-off "set and forget."

Cyber should be included in a business' overall risk mitigation programs and policies. As we have said before, cyber risk is a business risk not just a technology problem.

Cyber programs and policies should be dynamic, practiced and able to be evidenced. A static "tick the box" checklist is no longer the best of the breed.

There is much more to unpack with the ruling, but I hope this gives you a flavour of what has been happening in the world of financial advice.

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

www.bcyber.com.au

karen@bcyber.com.au

twitter.com/bcyber2

youtube.bcyber.com.au/2mux