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

Board Speak versus Tech Speak: same-same-different (really different)

Cyber risk is a key concern for boards today. They usually come at it from a non-technical background, and only a few IT professionals speak the language of business. So, we find ourselves at an impasse, or do we?

Things are made more confusing by the fact there are some terms with multiple meanings depending on the context, or even the industry the business operates in. To get you started, here are my top four terms you need to be mindful of. There are many more.

Asset Register You mean technology assets: business owned information systems or hardware.

They hear depreciation schedule and company assets: things the business owns and/or controls and uses.

Asset management You mean an inventory of all technology assets and tracking all "devices" that interact with your business and the internet to help you understand your attack surface.

They hear investment management, and they expect a focus on increasing the wealth of the business by acquiring or selling and/or managing investment assets.

Audit You mean a process that is part of (IT) asset management, or perhaps privileged asset management, or understanding what assets the business has, who has access to each asset, and why.

They hear (and possibly fear) financial audit and/or Australian Financial Services Audit, or a visit from the Australian Taxation Office for an ATO audit. Their interpretation will be industry specific.

Compliance You mean the business's digital security requirements and practices, be they legal requirements, a security standard, or a framework.

They hear industry specific requirements with possible fines or worse. For example, Australian Financial Services licensees have a multitude of legal obligations they must adhere to that cover everything from monitoring and supervising authorised representatives to complaints, compliance with the Anti-Money Laundering and Counter-Terrorism Financing Act, training, appropriate advice, mandated client reporting, and more.

So, next time you address a board or have that meeting with the accounting department to get financing for your new cyber resilience program, remember what you are saying may not be what they are hearing. It is up to us to change that.

BCYBER®

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

www.bcyber.com.au

karen@bcyber.com.au

twitter.com/bcyber2

youtube.bcyber.com.au/2mux