KAREN STEPHENS

Karen Stephens is the co-founder and CEO of BCyber. After more than 25 years in financial services, Karen moved into SME cybersecurity risk management. She works with SMEs to protect and grow their businesses by demystifying the technical aspects of cybersecurity and helping them to identify and address cybersecurity and governance risk gaps. She was recently named inaugural Female Cyber Leader of the Year at the 2023 CyberSecurity Connect Awards in Canberra.

COLUMN

Cybersecurity governance is key to business survival

In our little corner of the cyber world, we have been saying for years that *"cyber is more than just a tech problem, it's a business risk problem."* Strong cyber resilience is all about good governance and risk management; a rather controversial statement when, traditionally, cyber resilience has been all about the tech, with the focus on 'security in depth' and, more recently, 'security by design'. However, lately we have started to see a shift in attitude from some quarters.

So, let's unpack what some see as a rather scary world of 'cybersecurity governance': what it is, why it is important and how you can start taking a few small steps in the right direction.

WHAT IS CYBERSECURITY GOVERNANCE?

When all is said and done, it is simply the approach your business takes to manage your cyber risk as defined by your management team. Generally, it involves establishing and maintaining a framework, management structure and processes to address identified cyber risks.

IT SOUNDS LIKE A LOT OF EXTRA PAPERWORK FOR NO ROI.

The importance of cybersecurity governance lies in its role in preparing you for a cyber breach incident and providing you with the ability to demonstrate to your key stakeholders (clients, partners, investors, regulators, insurers, etc) your preparedness and resilience and ability to respond to cybersecurity incidents. In practice, it also means that, should a cyber incident occur, you know exactly what to do, and when and how to do it.

Establishing a cybersecurity governance program can seem somewhat overwhelming. So, here are two things you can do to get yours started today.

1. **Understand your cyber risk.** Complete a thorough cyber risk assessment of your business and communicate the most critical risks to the board. This includes understanding your threat landscape, identifying vulnerabilities and assessing the effectiveness of current cybersecurity tools in mitigating the identified risks. After this assessment, actions and monitoring tasks will be outlined and followed up, but that is for another day.

Special hint: *your cyber risk assessment will ensure you identify critical risks such as third-party vendors, and specific actions your business can undertake to mitigate any associated risks. Third-party risk is just one example of the many risks you will need to identify and address, but as it seems to be in the headlines at the moment, it's worth a special mention (let's give a shout out to Firstmac, IRESS, (which resulted in OneVue being affected) and MediSecure)*

2. **Written and practiced plans.** Develop comprehensive cyber breach response and business continuity plans to address any potential cyber incidents. These plans should be developed in collaboration with key stakeholders and should include a structured cyber breach response strategy, crisis management protocol and routine assessments of cyber risk status.

Special hint. *Build muscle memory by conducting regular run throughs of your cyber breach response and business continuity plans. You don't want the first time you open the plans to be in response to a live breach.*

Remember, good cyber governance is not a nice-to-have. It is a must-have, if you take your cyber resilience seriously.

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

www.bcyber.com.au

twitter.com/bcyber2

karen@bcyber.com.au

youtube.bcyber.com.au/2mux