Ignorance is no excuse for naïve CEO's

Boardrooms are a never-ending surprise of curious machinations – intertwined with interesting characters, they're not dissimilar to Forrest Gump's 'Box of Chocolates' - imbued with different offerings but interestingly bland in taste.

That's not to suggest all boards are the same, but it's not unrealistic to think many have similar offerings, creating scenarios of concern amongst businesses and Australians – operating like rudderless ships through stormy waters of misguided direction and belief.

Australia has an underlying problem with its corporate leaders, many lack vision and creative thought and are stuck in the mire of the past, stiff and unnameable like collars of over starched shirts.

Having a steady hand of caution, can also be a blocker to progress - in a modern world where technology challenges all that we do, the ability to think in waves of modernity is critical, which explains in part why corporate Australia faces increasing cyber-attacks and data breaches.

Boards and Australia’s leadership must become progressive thinkers and not remain immersed in business practices or thinking of the past. The world is a different place to what it was 40 years ago. We have evolved!

Security is not an IT issue. Security is an executive problem borne out of the naivety of corporate leaders who fail to understand what’s required to protect and safeguard our personal information against cyber-attacks or data breaches.

Failure by corporate leaders to understand how their inaction or ignorance around providing appropriate funding and infrastructure support to protect against cyber-attacks or data breaches, also poses a legal question about liability and that of the organisations failure to safeguard data.

Ignorance is no excuse as a defence in law, and many corporate leaders are walking a knifes edge from being sued by any person or corporation prepared to challenge the matter legally if the information another organisation is meant to be safeguarding is breached.

If Australia’s corporate leaders continue to choose to remain oblivious around data breaches and cyber-attacks, and not sure up their business’ defences, it won’t be too long before Pandora’s box is opened for a new era of litigation that could take years to resolve.

Research conducted around cybersecurity continues to repeat a disturbing theme of dire inevitability.

Recently released figures around the existence of the implementation of effective cyber security programs show two out of every five Australian companies have no strategic framework in place for cyber security planning, with close to 50% not providing staff with cyber awareness training programs.

Global research group, Gartner, in its most recent offering said, “By 2022, cyber-security ratings will become as important as credit ratings when assessing the risk of business relationships.”

The Cyber Assurance Risk Rating (CARR) initiative, launched in Australia in August this year, is now the default standard for managing this process and has businesses clamouring to use the service.

The Design Institute of Australia is one example of an organisation faced with the challenges of guarding against data breaches and cyberattacks which uses CARR.

As Australia’s peak industry body for professional design and representing Australian design and designers locally and abroad, it recognises the potential risk of cyberattacks the organisation faces. What it holds is the intellectual property and design concepts on a broad range of initiatives or highly confidential programs an individual, business or industry may be involved in, and what it contemplates is how it insures against and manages any attacks.

The DIA now sits comfortably knowing as an organisation, it has begun to put in place the necessary mechanisms of protection.

What CARR provides organisations, from the legal profession onwards, is the ability for companies to obtain a score, identify strengths and weaknesses of their own systems, partners, vendors or acquisition targets.

Astonishing as the world has become and continues to be, knowing and understanding the real threat and dangers cyberattacks pose in an environment where evolution is just the blink of an eye, is corporate Australia's underwhelming preparedness to tackle these challenges and threats.

It would be reasonable to describe the leadership of corporate Australia as disturbingly negligent and irresponsible, especially when research figures reveal an incredible 86% of Australian companies never having reviewed the Cyber Security practices of their business partners.

PageUp, the Australian Blood Service or NSW Family Planning are but three examples of major significant data breaches which potentially ran the risk of jeopardising the privacy of its clientele. A review may have contributed to a better, complete understanding of the security risks they faced or were threatened with.

Knowing where risk comes from provides significant benefits – it allows for better decision making. It provides auditability, clear metrics and a safer organisation in the digital wolrd.

It makes sense to guard against the unknown and the dangers that lay within the murky realms of the cyberworld, but to stop the legal hounds from baying.

Authored by

Michael Connory

Michael Connory is the CEO of Security In depth.