CEO’s playing Russian Roulette with Aussies personal data

Russian Roulette is an interesting game of dare, jockeying against chance. One bullet in a six-barrel chamber hoping the squeeze of the trigger isn’t a fatal shot.

It’s an unintended death wish of the naïve failing to comprehend the consequences of the game they play.

Russian Roulette is what Australian Businesses are playing with our data. It is abundantly clear they fail to understand cybersecurity and the new world now under construction.

Australians live in a different world to circa 2000. Our bubble of protection is now an open fissure for any who dares to enter the rabbit warren into Alice's Wonderland and seek to discover what they can.

Two thousand and eighteen has shaped a new world, a frontier where privacy in some accidental fashion is no longer our own. The custodians of all we consider sacred, have failed our trust - not through sinister intent, but through naivety and compromise for the sake of minimising expenditure and investment.

The release of the OAIC Notifiable Data Breaches Second Quarterly Report last week, revealed disturbing trends around the security of our information and what value is placed on its protection – none it seems!

As harsh a comment it maybe, valuing protection can only ever be measured by commitment to invest in initiatives to ensure its safeguard.

Information into our lives and who we are and what we do, is now a biddable auction given the failure by Australian Businesses to secure our data.

The OAIC's Report, is a damning condemnation surrounding businesses failure to protect the privacy of Australians and the information held on us.

It shows an alarming number of data breaches throughout June, were due to human error or phishing attacks, which is not a surprise. For all the rhetoric we hear about data protection, it seems actions are failing to marry to the words that are spoken.

Through investment, reducing data breaches can be managed with the right level of cybersecurity training, not just buying more technology.

Human error is the primary contributing factor behind data breaches and why they occur. Thirty-six percent were reported last quarter, which could have been prevented.

What was preventable, has been a tinkering around the edges - a piece-meal attempt to satisfy legislative requirements.

During the March quarter, over 1 million Australians were impacted by data breaches - 90 reported in June were more than the first quarter combined:

1.
    1. 42% involved your personal financial information
    2. 39% identity theft – your drivers licence details, your passport details, your home address and your date of birth could have been lost
    3. 19% Tax File Number – add this to Identity theft and a person's entire financial future is at risk

Statistics paint a picture of many sorts – Security In depth's most recent research supports many of the OAIC findings. The canvass we paint is despairing:

- 75% of breaches over the last three months directly relate to staff error

- Organisations have increased spending on Cyber technology by 7% in the last financial year – mostly the top end of town
- 70% have not increased investment in security
- Security specialisation within Corporate Australia rose only 2% - with most security specialists being employed by either Government or multi-nationals
- 85% of companies don't have a dedicated security staff member
- 91% of ICT staff still attest to difficulty with management's reluctance to increase spending on cybersecurity in 2018
- 42% of all companies have no security framework. No policies, no procedures, no governance
- 35% using basic security practices like those recommended by the ASD (Australian Signals directorate)

Significant failure exists in Governance – 63% of businesses have no security awareness training and 65% of security personnel work for the CIO – this leads to technology-based solutions rather than good governance.

Corporate Australia is not taking cybersecurity seriously. The statistics are a bewildering tale, most disturbing is the evidence around how many Australian companies and businesses choose to roll the dice and play their version of Russian Roulette and their willingness to gamble with our privacy.

The numbers will increase, the costs for managing cyber Incidents will continue to escalate out of control, and we are yet to see the true residual damage incurred to individuals who have been impacted by a breach.

Disturbing above all is the belief by Boards around cybersecurity that investing in technology is all that is required to protect the assets they hold – client data information.

Rolling the dice on, and hoping against the odds there won't be security breaches is fascinating, especially when the investment to protect against breaches have not been made, begging the question, will we be hit? We may not, but the reality is, it's an unknown event that potentially bares dire consequences– just like the single bullet in a six-barrel chamber.

Michael Connory is the CEO of Security In depth.