THE AUSTRALIAN

Business playing Russian roulette with cybersecurity

By **MICHAEL CONNORY**
52 MINUTES AGO AUGUST 7, 2018 • NO COMMENTS

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.

And that's exactly what Australian businesses are playing with our data.

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 as it may be, valuing protection can only ever be measured by commitment to invest in initiatives to ensure its safeguard. Information into our lives is now a biddable auction given the failure by 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 that 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 per cent were reported last quarter, which could have been prevented.

What was preventable has been a tinkering around the edges — a piecemeal attempt to satisfy legislative requirements.

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

● 42 per cent involved your personal financial information;

● 39 per cent identity theft — your driver's licence details, your passport details, your home address and your date of birth could have been lost; and

● 19 per cent 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's findings. The canvas we paint is despairing:

• 75 per cent of breaches over the past three months directly relate to staff error;

• Organisations have increased spending on cyber technology by 7 per cent in the last financial year — mostly the top end of town;

• 70 per cent have not increased investment in security;

• Security specialisation within corporate Australia rose only 2 per cent — with most security specialists being employed by either government or multinationals;

• 85 per cent of companies don't have a dedicated security staff member;

• 91 per cent of ICT staff still attest to difficulty with management's reluctance to increase spending on cybersecurity in 2018;

• 42 per cent of all companies have no security framework. No policies, no procedures, no governance; and

• 35 per cent use basic security practices like those recommended by the Australian Signals Directorate.

Significant failure exists in governance — 63 per cent of businesses have no security awareness training and 65 per cent 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 incidents will continue to escalate out of control, and we are yet to see the true residual damage incurred to individuals who have been affected 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 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 CEO of Security In Depth.