THE AUSTRALIAN

Corporate Australia under lock and key

Michael Connory, CEO of Security in Depth. Picture: Supplied

MICHAEL CONNORY THE AUSTRALIAN 12:00AM March 27, 2018

There was a time when securing information and storing it was an easy process. It required classifying documents and files in alphabetical order or by subject, loading them into cabinets and securing them under lock and key.

What a simple world it was.

But the world we now live in is a complicated place with data and cybersecurity a key part of all that governs the way organisations function. The evolution of technology means cybersecurity and storage brings with it legal governance and protocols necessary to protect the privacy of the data.

Corporate and government organisations are the keepers of all big data stored in a cyber world. The expectation is, as big data continues to get bigger, cybersecurity and governance gets tighter and tighter.

Like the solid granite wall perimeter and squads of armed guards surrounding Fort Knox, along with its 22-tonne vault blast door and intricate locking systems, its integrity has never been challenged, and that's how the security of organisational data store should resemble, or so we would like to think.

How is it that those charged with protecting our information seem to have very little idea of the programs and governance controls required to secure the data they keep?

Governance is a word that consistently appears as part of the modern lexicon. It is corporate speak for procedures ensuring businesses behave in a manner compliant to corporation laws and standards, or to ensure a predefined outcome — such as the security of information and systems.

In a recent survey conducted of more than 973 of Australia's business leaders, we discovered a disturbing level of complacency on the issue of cybersecurity and the protection of data.

One surprise finding of our survey was the lack of concern ascribed by respondents that a major breach could impact on the reputation of their organisation. It's crazy to think Australia's corporations and its leaders are flying blind in a haze of misconception.

The statistics are way too confronting to ignore. Perched on the precipice of the threat of a breach, is the threat of financial fallouts and legal suits that are likely to follow — protecting the highly valuable and sensitive data corporate Australia and its governments are entrusted with, should be the key premise that motivates the use of carefully designed defences, the digital equivalent of those physically deployed at Fort Knox.

Almost 77 per cent of the organisations surveyed across Australia have no governance program that addresses cybersecurity.

This translates into a significant failure of policies and procedures to ensure information is treated and protected appropriately.

Furthermore, a staggering 28 per cent of ICT staff, (CIOs and CISOs) surveyed expressed the opinion that their companies are secure across the same demographic — a clear example of the extent of the cybersecurity problems at play within the operational and security management machinery of Australian businesses.

About 44 per cent of CEOs and CFOs believe their organisation's ICT network are adequately secured whereas 37 per cent believe their network was highly secured.

Creating a platform change to address the transition from internally to externally available systems requires drastically different thinking, adopting a new strategic approach to the problem around enacting proper cybersecurity protocols.

As simple as it seems, the challenges facing executives is the provision of additional funding to ensure this transformation is fully achieved. While 62 per cent of businesses surveyed reported an increase in IT-related funding. However, it does not appear this funding was being applied to addressing key weaknesses in cybersecurity capability. For example, reported funding increases did not appear to provide address for the following:

• qualified cybersecurity staff — at least 78 per cent claim one more qualified staff was required

• investment in strategic responses — 58 per cent assert that funded security activities are tactical, not strategic.

Hole plugging isn't exactly a remedy that beds down the issue around ensuring an organisation is secure, rather it exposes the threat of dozens of others.

A poll conducted with CEOs of Australia's manufacturing sector sought to understand whether they had a plan in place to manage a data breach — 68 per cent claimed they had no plans or even considered enacting a plan, while 19 per cent said they were organising an appropriate incident response plan later in the year.

Corporate Australia is entrusted with information we value highly. The expectation of preparation is a demand that must be adhered to. And as Benjamin Franklin, inventor, polymath, scientist, and a founding father of the US said: "By failing to prepare, you are preparing to fail."

Michael Connory is the CEO of Security In Depth.

EXCLUSIVE

Airmow gains a cutting edge

DAVID SWAN

Australia has its first on-demand marketplace for lawnmowing.

FOUR PILLARS

Narev team continues to unravel

RICHARD GLUYAS

The unravelling of CBA chief executive Ian Narev's hand-picked leadership team has been extraordinary.

More CBA execs shown the door

MICHAEL RODDAN

More senior executives will leave the Commonwealth Bank in the wake of the money laundering scandal.

Harvey's dairy venture turns sour

ELI GREENBLAT

Gerry Harvey's dreams of creating a thriving dairy empire have soured.

FAR nears offshore drilling success

MATT CHAMBERS

FAR is closer to recognition for leading the most successful offshore oil campaign by an Australian company this decade.

Smith scratched from Weet-Bix

SIMONE ZIAZARIS, STUART CONDIE

The Australian cricket captain is no longer visible on Weet-Bix's website following the ball-tampering scandal.

Back to top