New data breach laws a potential honey

POLITICS | 20 JUNE 2018 | MICHAEL CONNORY

Corporate Australia is in a bind of enveloped misconception, and it may be the lawyers who win the day, writes **Michael Connory**.

Caught between progression and changing landscapes, technology has evolved rapidly for even the most advanced corporates to keep ahead of the game. Among it all, the change and evolution of growing security breaches remain an ongoing threat to the privacy of every corporate's clients.

The world of business today is a canvas painted of di erent colours and hues to that of decades ago.

Data protection is a key issue for corporate Australia, and how it chooses to safeguard privacy has become a contentious issue with new legislation enacted to ensure stricter measures and protocols are adhered to.

As much as the federal government has legislated new data breach laws, there remains a small number who have adopted these changes while others are failing to understand the new laws are a two-way street – to protect the information of all Australians that corporates hold and to help corporate Australia safeguard themselves against potential future litigation.

Adaptation is the implementation of change required to meet the demands of evolving times.

Change requires com mitment to move ahead, which means if corporate Australia fails to cater for the new mandatory data breach laws introduced, will there be an increase in the number of organisations facing litigation?

Lawyers Weekly (/)

In the four months since their introduction, 60 breaches were communicated directly with the O ice of the Australian Information Commissioner within the first few weeks of legislation a ected.

In addition to these breaches we have also seen:

- The Commonwealth Bank's loss of 19 million of its customers financial
- records; Family Planning NSW's the of the records of 8,000 women;
- A ransomware attack on so ware objective, shutting down the system for many in the building industry; and
- PageUp, potentially impacting on 2.9 million individuals a er threats of cyber attacks were monitored within their system.

They are just some of the attacks that have occurred in the short life span of the new data breach laws coming into play.

With the recent cyber attacks mentioned, interesting questions remain; will there be a rise in legal suits against companies for breach of duty of care, and what will be considered as reasonable steps for an organisation to take to protect client information?

And if this is to be the case, then the size of the suits could be a honey pot of gold, of which lawyers will earn a sizeable share.

Will better technology be the key to resolving what could be an enduring problem, and if so, what occurs when a system is attacked that does

not patch legacy application? Or could conducting reviews on suppliers that integrate with systems be the answer?

Recent research conducted by Security In depth revealed a staggering 7 per cent of companies currently complete this process. It's a small number that paints a damning picture of the fate that awaits corporate Australia, and how lawyers are destined to reap the spoils of what could unfold.

At the end of 2017 and early this year, Security In Depth conducted its 'Cyber Security in Australia Project' survey.

What the 9,118 companies surveyed across Australia showed was a enlightening look into how they have been preparing for the new data breach laws, and what was unearthed was a frightening tale of misadventure and darkness looming over the horizon for those companies who had no strategy in play to deal with the new laws.

It found a disturbing:

- 7 per cent of organisations fully reviewed suppliers integrating or managing
- internal ICT systems. 11 per cent of organisations had a fully tested incident
- response plan in place for a data breach and 22 per cent Australia-wide had conducted cyber awareness training for their sta

Since the introduction of the 22 February data breach laws, Security In Depth has seen an incredible 1 per cent increase with organisations instigating third-party reviews of security systems, a 6 per cent increase with organisations having a fully tested incident response plan in place for a data breach to 17 per cent, which is still inadequate.

Furthermore, there amount of organisations across Australia who were conducting cyber awareness training for their sta rose from 22 per cent to 37 per cent, but these figures still reflect continued low numbers.

Statistics always tell an interesting story, and the greatest story told is the estimated 33 per cent of Australian businesses experiencing a cyber crime, according to PwC and the Ponemon Institute - more than 114,000 instances of cyber crime have been reported over the last three years.

And when a cyber event is experienced, what steps have companies taken to ensure they have not been negligent

with their duty of care? Very little it seems.

That for many companies will be the multimillion-dollar question that they could face during litigation.

Michael Connory is the CEO of Security In Depth.
