Mandatory data breach laws a potential honey pot for lawyers

Will there be a rise in legal suits against companies for breach of duty of care?

Michael Connory (CIO) | **19 June, 2018 11:33**

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

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

The world of business today is a canvas painted of different 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.

Some organisations have adhered to these changes to data privacy laws while others are failing to understand that they are a two-way street; they protect the personal information of all Australians that organisations hold while helping these companies safeguard themselves against potential litigation.

Adaption is the implementation of change required to meet the demands of evolving times. Change requires commitment 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?

Within the first few weeks of the legislation coming into effect in February, 60 breaches were communicated directly with the Office of the Australian Information Commissioner.

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 theft of the records of 8000 women;
- A ransomware attack on Software Objective, shutting down the system for many in the building industry and;
- PageUp, potentially impacting on 2.9 million individuals after threats of cyberattacks were monitored within its systems.

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, 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 which lawyers will earn a sizeable share. Will better technology be the key to resolving what could be an enduring problem? If so, what occurs when company is attacked and its legacy applications have not been patched?

Could conducting reviews on suppliers that integrate with systems be the answer? Security In depth's recent 'Cyber Security in Australia Project' survey with executives at 9,118 companies found that 7 per cent currently completed this process.

It's a small number that paints a damning picture of the fate that awaits organisations across Australia and how lawyers are destined to reap the spoils of what could unfold.

Security in Depth's research unearthed 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 that only 11 per cent had a fully tested incident response plan in place for a data breach; and only 37 per cent has conducted cyber awareness training for their staff.

Statistics always tell an interesting story, and the greatest story told is that more than 114,000 instances of cybercrime have been reported over the last three years, according to PwC and the Ponemon Institute.

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 millions of dollar question that they could face during litigation.

Michael Connory is the CEO of Security in Depth.
