

What should Australian companies be doing right now to protect our privacy

Written by The Conversation

Australians are increasingly concerned about how companies handle their [personal data](#) , especially online.

Faced with the increasing likelihood that this data will be compromised, either through cyber attacks or mishandling, companies are now being forced into a more comprehensive approach to collecting and protecting customers' personal data. The question remains - what is the best approach to achieving this goal?

The Organisation for Economic Co-operation and Development (OECD) has proposed that instead of talking about cybersecurity - companies, organisations and nations should be viewing the problem from a [digital security risk management](#) perspective.

Cybersecurity often overlooks risks to data that have nothing to do with a “cyber” element, even if people could agree on a definition of that term. In the case of Edward Snowden for example, he [used](#) a colleague's credentials to access the system and copied files to a [USB drive](#) .

Digital security risk management involves getting everyone in an organisation to see digital risk as part of the overall risks that the organisation faces. The extent of risk any organisation is willing to take in any particular activity depends on the activities value. The aim is to manage the risk to a level that is acceptable to all parties.

What do you do about the weak link: humans?

It is worth remembering that in the case of the [Equifax breach](#) in which the personal details of up to 143 million customers in the US were leaked, it was largely human errors that were to blame.

Put simply, the [person](#) who was responsible for applying the patch (a piece of software designed to update a computer program or its supporting data, to fix or improve it) simply didn't do their job. The software that was supposed to check whether the patch had been applied also failed to pick this up.

Until humans can be taken out of the equation entirely, it is almost impossible to remain entirely secure, or to avoid the inadvertent disclosure of personal and private information. [Insider threat](#) (as this type of risk is known) is difficult to combat and companies have tried various [approaches](#) to managing this risk including predictions based on psychological profiling of staff.

Automation and artificial intelligence may be a way of achieving this in the future. This works by minimising the amount of sensitive information staff have direct access to and surfacing only the analysis or interpretation of that data.

A litany of recent breaches

If you needed convincing about the vulnerability of personal data on the Internet, you only need look at Gemalto's data breach [website](#) or [DataBreaches.net](#).

The breaches of private and personal information don't recognise national boundaries with hacks of companies like Yahoo [having affected](#) 3 billion users, including millions of Australians.

Of course, Australian companies and organisations have also been involved with spectacular data breaches. Last year saw the Australian Red Cross [expose](#) 555,000 customer records online.

Of more concern was the Australian Department of Health had [published](#) online what they believed were de-identified records of Medicare and pharmaceutical claims of more than 3 million patients. Researchers at the University of Melbourne discovered that the "encrypted" doctor provider numbers could be decrypted.

Are we looking at it in the wrong way?

Whilst there are practical steps companies can take to protect digital systems and data, there are more fundamental questions companies should be asking from a risk perspective. In order to navigate these questions, companies need to understand the data they collect and perhaps surprisingly, this is something [most companies struggle to do](#).

What should Australian companies be doing right now to protect our privacy

Written by The Conversation

The 13 [Australian Privacy Principles](#) from the Office of the Australian Information Commissioner outline the basics of how organisations and agencies should handle personal information. The practical [application](#) of these principles involves an approach called Privacy By Design for all applications and services companies offer.

Enter confidential computing

For CSIRO's Data61, the [answer](#) to breaches of this sort is "confidential computing". [Data61](#) is tasked with data innovation and commercialisation of its research ideas. Confidential computing is the remit of Data61's latest spin-off, [N1 Analytics](#).

The main aspect of confidential computing involves keeping data encrypted at all times and using special techniques to be able to query data that is still encrypted and only decrypting the answer.

This can even allow others outside an organisation to query internal data directly or link to it with their own data without revealing the actual underlying data to either party.

Aside from the case of allowing the use of sensitive data in research, this approach would allow a company with financial information say, to share this data with an insurance company without handing over sensitive information but theoretically letting the insurance company carry out extensive data analytics.

What companies should do now to protect your data

As a starting point, Australian companies should only collect the minimum of personal information that the business actually needs. This means not collecting extra information simply for marketing purposes at some later date for example.

Companies then need to explain in simple, clear, terms why information is being collected, what it is being used for and get users to consent to giving that information.

What should Australian companies be doing right now to protect our privacy

Written by The Conversation

Companies then need to secure the data that is collected. Security involves dedicated staff understanding the data that is kept by a company and taking responsibility for its physical security and for controlling who has access, when they have access and what form they can access the data.

Lastly, they need to understand and enact a risk management approach to all digital data. This means that this is part of the overall culture of the company for every employee.

David Glance consults for the OECD on digital security risk management.

Read more <http://theconversation.com/what-should-australian-companies-be-doing-right-now-to-protect-our-privacy-85247>