Questions still need answering in Australia's largest health data breach

October 31 2016, by David Glance

In what is Australia's biggest data breach of medical information, more than 550,000 customers of the Australian Red Cross Blood Service had personal and medical details exposed online and leaked to an anonymous hacker last week.

According to the Blood Service, the data leaked was contained in a backup of a database of its online web site. One part of the database contained the answers to an online questionnaire which donors complete in order to book an appointment with the service. The questionnaire covers information about the donor's name, age and address but also medical questions related to the donor's current health, state of pregnancy and finally about whether the donor has in the last 12 months, engaged in at-risk sexual behaviour.

The backup database had been left, not on the Blood Service website, but on a server managed by the Blood Services's website developer, Precedent. The database was found there by an anonymous hacker who had been scanning sites for security vulnerabilities and stumbled across the completely unprotected database.

On realising what the data was, the hacker contacted a consultant, Troy Hunt, who runs a site called "have i been pwned". Have i been pwned allows people to see if their email address and other details have been leaked and made publicly available in previous data breaches. Hunt's and his wife's details were included in the Blood Service database because they had both donated blood in Australia. Hunt contacted AusCert, a

cyber emergency response team located at the University of Queensland and informed them of the breach and the data he had been sent.

AusCert in turn contacted the Blood Service who then notified its donors of the breach. Hunt and the anonymous hacker both deleted their copies of the backup database. Security specialists the Blood Service had employed to review the breach determined it was likely the database had not been discovered by anyone else in the time it was available on the internet.

For the time being, it looks like the Blood Service has managed to dodge what could have been an even more devastating blow to its credibility. While most donors (including Troy Hunt) may not let this incident stop them from donating in future, the incident does bring into question the overall capability of the Blood Service to protect and keep safe extremely sensitive information about its customers. A question it should be addressing is why it was collecting and saving this information through its website in this manner in the first place. An even bigger question is whether it will continue to collect and save this information in the same way.

What the Blood Service should be asking itself is:

1. Do I really need to collect this information? In the case of the Blood Service the answer is probably no. While it seems like it is being efficient to ask screening questions on the appointment questionnaire, none of the information needs to be saved if the point is simply to give feedback to people that they are unlikely to be eligible to donate blood.
2. Do you know where all of your data is? In the case of the Blood Service, and indeed its contractor Precedent, the answer was clearly no. A developer had taken a backup of the live system which he or she shouldn't have needed access to, and put it on an

unsecured server that was exposed to the internet. Considering the type of sensitive information the Blood Service dealt with, to entrust that information to a web developer without putting any checks or process in place to prevent access to this information highlights the inexperience of the Blood Service.

3. Do you know who has access to all of your data? Again, the Blood Service clearly didn't know that developers at Precedent would have access to its production data. Given this data was unencrypted, it meant people outside of the Blood Service would have had the ability to look at the data and potentially leak this information through informal channels. A developer or other staff member at Precedent could have searched the data for a relation, friend, colleague or celebrity to see if they had engaged in risky sex, for example. There seemed to be no protections built into the website itself to manage or restrict access. This is possibly because the Blood Service didn't treat the questionnaire as part of its core systems, erroneously trying to reassure donors that: "The website forms used to collect this information do not connect to our secure internal databases which contain more sensitive donor medical information". The Blood Service clearly felt, incorrectly, that the personal information collected as part of the questionnaire was not sensitive.

There are of course, more direct cyber security measures that need to be implemented but they are of little use if a company isn't even aware of the fact they have data that needs protecting.

By comparison with the US, this data breach is still moderate. A hack earlier this year of 21st Century Oncology affected 2.2 million patients. Another case this year saw details of 950,000 of Centene's patients lost on six computer hard drives.

In the US, 21st Century Oncology is facing a US $57 million class action

lawsuit over the breach. US federal regulators recently fined Advocate Health Care Network US $5.55 million over three separate breaches that could have affected 4.1 million patients.

The Australian Red Cross Blood Service, and its contractor Precedent, potentially face fines of up to AU $1.7 million for this breach if it is deemed to have violated the Privacy Act. In the past however, Australian telco Telstra was fined a mere AU $10,000 for exposing the details of 16,000 of its customers online.

If the Blood Service continues with the questionnaire for appointments on its website, it will be clear it hasn't learned any lessons from this breach. Precedent in turn, needs to demonstrate to the Blood Service and all of its other clients that it actually can live up to its privacy statement which says: "We store your information securely on our computer system, we restrict access to those who have a need to know, and we train our staff in handling the information securely."

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation