Red Cross Blood Service partner owns up to data breach blunder

Investigation report reveals employee mistake

Leon Spencer (ARN) | **07 August, 2017 12:07**

It has been revealed that a Precedent Communications employee was behind the massive data breach that hit the Australian Red Cross Blood Service late last year.

According to a pair of new investigation reports into the breach, published by the Office of the Australian Information Commissioner (OAIC) on 7 August, a backup of a database file containing information relating to approximately 550,000 prospective blood donors was inadvertently saved to a public-facing web server by an employee of the IT partner on 5 September 2016.

It wasn't until almost eight weeks later that the data file was discovered and accessed by an unknown individual, on 25 October 2016. On the same day, that individual notified the Blood Service via a number of intermediaries.

The Blood Service immediately took steps to contain the breach.

In the aftermath of the breach's discovery and mop-up, Rob Van Selm, the Asia Pacific managing director for Precedent – as a Blood Service partner – confirmed only that the company was working with the organisation in relation to the breach, but offered no further detail on the company's involvement.

Precedent Communications is a digital agency with offices in Perth and Melbourne, and further afield in areas such as London and Hong Kong. It provides services, including technical development and support, for clients' websites.

In 2014, the company was awarded the contract to re-develop the Blood Service's desktop and mobile Donate Blood websites into one platform with additional capabilities.

After the new Donate Blood website was launched in 2015, Precedent was also awarded the contract for the Donate Blood website development and application support, ongoing management, consulting and testing, and maintenance and upgrades.

Now, thanks to the investigation and its subsequent reports, the company's role in the breach, and its subsequent remediation activities, have become clearer.

At the time of the incident, according to the report, information entered by potential donors remained on the back-end of the Donate Blood website, as well as being transmitted to the Blood Service.

The production environment of the website was hosted for Precedent by Amazon Web Services. Non-production environments, including the website's User Acceptance Testing (UAT) environment were hosted and managed by Precedent directly.

That UAT environment held a copy of the website, including customer data which was 'refreshed' on a monthly basis. It contained a copy of all data entered into the production version of the Donate Blood website.

The actual UAT environment was protected by Precedent through a number of mechanisms, according to the report. However, portions of the web server on which the UAT environment was located were publicly accessible, the report into Precedent's involvement in the breach stated.

On 5 September 2016, the unnamed Precedent employee who was tasked with enhancing a feature on the Donate Blood website created a database backup of the UAT database file (the data file) on the UAT environment before making changes to the system.

"The backup would have allowed for the restoration of data should an error occur during development work or database upgrades," the report stated. "The employee had intended to save the data file created to a secure location but, in error, saved the data file to a publicly accessible portion of the web server on which the UAT environment was implemented."

The data file in question contained registration information of the 550,000 prospective donors who requested an appointment to donate blood via the website between 2010 and 5 September 2016. It is understood that the breach potentially involved more than 1.28 million records.

The data file included the personal information of individuals who had expressed an interest in donating blood on the Donate Blood website.

It also included sensitive information about some of the individuals, including first and last name, gender, physical address, email address and phone number, and yes or no responses to donor eligibility questions such as whether or not the prospective donor had engaged in risky sexual behavior.

The investigation into the breach and the subsequent report by the OAIC concedes that the Precedent employee's mistake was the cause of the breach and that it did, indeed, constitute a "disclosure".

"The root cause of the data breach was an unforeseen one-off human error on the part of a Precedent employee," the report said. "However, the error was made in the course of that individual's duties, and as such the data breach was a 'disclosure' within the meaning of Australian Privacy Principle (APP) 6," – which outlines when an APP entity may use or disclose personal information.

According to the OAIC, Precedent breached the Privacy Act in respect of APP 6 and APP 11 – which requires an APP entity to take active measures to ensure the security of personal information it holds – by disclosing the personal information of individuals who had made an appointment on the Donate Blood website, and for failing to take reasonable steps to adequately mitigate against the risk of a data breach.

"Although Precedent had not met all the requirements of the Privacy Act, the Commissioner acknowledges Precedent's constructive and cooperative approach in working with the OAIC in this matter," the report stated.

In response to the incident and its fallout, Precedent has subsequently invested "significant effort" to improve its information handling practices, strengthen its information security, and ensure that it is now compliant with the Privacy Act.

"To assure the Commissioner and the Australian community that Precedent will address the issues identified in the investigation, Precedent offered, and the Commissioner accepted, an enforceable undertaking on 28 July 2017," it said.

At the same time, the OAIC found that the data breach occurred without the authorisation or direct involvement of the Blood Service, and was outside the scope of Precedent's contractual obligations to the Blood Service.

As such, there was no "disclosure" by the Blood Service of the data file.

"The steps the Blood Service had in place to protect personal information at the time of the breach were, for the most part, adequate," the investigation report into the Blood Service's involvement in the breach stated.

However, the OAIC found that the Blood Service had breached APP 11, "in respect of the information on the Donate Blood website by retaining the information indefinitely, and by not having appropriate measures in place to protect information concurrently held by third party contractors".

Regardless, the Australian Information and Privacy Commissioner, Timothy Pilgrim, has suggested that the community can have "confidence" in the Australian Red Cross Blood Service's commitment to the security of their personal information, following his investigation.

"Data breaches can still happen in the best organisations - and I think Australians can be assured by how the Red Cross Blood Service responded to this event," Pilgrim said. "They have been honest with the public, upfront with my office, and have taken full responsibility at every step of this process."

The Blood Service has enhanced its information handling practices since the incident, and has provided assurance to the Commissioner through an enforceable undertaking, as has Precedent Communications.

For its part, Precedent proposed a set of measures to enhance its protection of personal information, and the Commissioner accepted the enforceable undertaking from Precedent, formalising its commitment to implement the measures within a specified timeframe.

"Based on Precedent's ongoing implementation of the measures proposed to enhance its protection of personal information, the Commissioner considers this an appropriate conclusion to the investigation," the report stated.
