

February 2019, Data breach example:

Bunnings exposed staff performance database

By [Juha Saarinen](#) on Feb 6, 2019 2:38PM

ITNews , www.itnews.com

https://www.itnews.com.au/news/bunnings-exposed-staff-performance-database-518929?eid=1&edate=20190207&utm_source=20190207_AM&utm_medium=newsletter&utm_campaign=daily_newsletter



Individual staffer did unwanted homework.

Bunnings has confirmed it notified the Office of the Australian Information Commissioner of a data breach, after an individual staffer set up an employee performance monitoring database on his home computer and exposed it to the internet.

The information in the database related to a single Bunnings store and was not hosted on internal systems, a spokesperson for the hardware retail chain told *iTnews*.

It was accessible over the web, and contained staff and customer information.

Lee Johnstone of security firm CTRLBox reported the data breach to Bunnings managing director Michael Schneider on January 30 this year.

Within hours of the report to Schneider, the database was taken down.

Johnstone told *iTnews* that the MySQL database was discovered by another researcher who wished to remain anonymous.

A limited number of Bunnings staff member details such as names and internal identification numbers were in the database, along with comments on employee performance. Most of the comments were positive, Johnstone noted.

The database also contained log in credentials for staff and developers, some in plain text, he added.

Furthermore, contact details of 1194 customers were exposed, including email and physical addresses, and phone numbers.

While he had no evidence pointing to unauthorised access to the database, Johnstone could not discount the possibility completely.

"It was a a public hosted IP [internet protocol address] so no doubt it was indexed by Shodan [a vulnerability search engine]," Johnstone said.

The spokesperson for Bunnings said the company was not aware of any malicious access to the database.

Schneider explained in a statement that the database was created by a Bunnings team member as an administration tool, and to assist in keeping local customers updated about activities and events.

Doing so however was a breach of Bunnings' data policy guidelines, Schneider said, and apologised for what has happened.

Bunnings will reinforce its data and privacy policies with staff to prevent future data leaks like the above.

The company has also begun contacting customers and employees affected by the data breach, Schneider said.