Uber hack: More than 1 in 10 Australians may be victims of Uber's 'astonishing' data breach

Jennifer Dudley-Nicholson, National Technology Editor, News Corp Australia Network

November 22, 2017

MORE than one in 10 Australians almost certainly had their personal information stolen by criminals in an "astonishing" hack on Uber accounts that the ride-sharing giant covered up for more than a year.

The multibillion-dollar company revealed the information of 57 million customers and drivers had been compromised in the data theft, which it then tried to cover up by paying a $US100,000 ransom to the perpetrators in a move new chief executive Dara Khosrowshahi admitted "should not have happened".

And tonight, Uber confirmed Australian customers' personal information had been stolen in the hack and informed the Privacy Commissioner.

The Uber security breach exposed its customers' names, email addresses, and mobile phone numbers, as well as the names and licence numbers of thousands of drivers that were stored with a third-party cloud service.

More than 2.69 million Australians use the ride-sharing service, according to Roy Morgan figures, or 14 per cent of the population.

The cybersecurity failure was exposed just months before new Australians laws force companies to reveal data breaches to consumers, though exclusive research from ESET will on Thursday reveal 60 per cent of organisations did not plan to reveal data thefts immediately.

An Uber spokesman did not confirm whether Australians were among the 50 million customers and 7 million drivers who had personal information stolen in the attack, but said the company was working to belatedly notify government agencies.

"We are in the process of notifying various regulatory and government authorities and we expect to have ongoing discussions with them," the spokesman said.

"Until we complete that process we aren't in a position to get into any more details."

Uber said no financial information or trip records had been stolen in the breach, but Mr Khosrowshahi said its "failure to notify affected individuals or regulators," and ransom payment prompted him to fire chief security officer Joe Sullivan and deputy Craig Clark.

"None of this should have happened and I will not make excuses for it," Mr Kosrowshahi said in a statement.

"We are changing the way we do business … and working hard to earn the trust of our customers."

Uber's data theft and subsequent cover-up would have put the company in breach of Australia's forthcoming "notifiable data breaches" law, due on February 23, which will force organisations to contact victims and report the theft of personal information to the Australian Privacy Commissioner.

But cybersecurity firm ESET will today reveal new research showing three in five Australian organisations were still not prepared to report cybersecurity breaches immediately.

The research, from a survey of 600 IT professionals, also found one in five either had not heard of the Privacy Amendment or did not know if they would be affected by the new law.

Sense of Security chief technology officer Jason Edelstein said greater attention needed to be paid to "properly" enforcing the regulations when introduced, as having even basic personal information stolen could have dire consequences for consumers.

"Names, email addresses and phone numbers leave Uber's riders or drivers susceptible to phishing attacks from these criminals. Driver's licence numbers is an even bigger issue as this could quite easily lead to fraud and identity theft," he said.

"It's an astonishing breach of its customers' privacy and will hurt the brand."

Mr Edelstein warned Australian Uber users to change their password as a preventive measure, carefully scrutinise messages purporting to come from Uber, and avoid opening email attachments from the company.