Medibank Data Breach – all data released
News story broadcast on Channel 7's "The Latest News"
1 December 2022
With Dr John Selby, Senior Consultant Privcore

Host introduction:
The worst fears are being realised for the 9.7 Million Australians caught up in the Medibank hack. The cyber-criminals behind it say that they have posted all of the remaining data with the message "Case Closed". Medibank says its own investigation is very much open. The company is going through the latest release to find out exactly what information has been exposed. Live from Melbourne is cybersecurity expert from consulting firm, Privcore, Dr John Selby.

Host: Does this latest drop mean the hackers have given up on a ransom - they're just aiming to inflict as much damage as possible?

Dr Selby: The hackers are focused on their long-term profits – whilst it seems they have given up on a ransom from Medibank, they want to motivate future targets to pay ransoms by showing how willing they are to cause harm to individual customers. Although their latest release has been of raw data, there is little to stop the attackers from investing resources to make that raw data easier to comprehend in future releases.

Host: For those customers who have been exposed - if they see their information circulating on the internet, is there anything they can do?

Dr Selby: Affected individuals should take steps to protect their identities, particularly using multi-factor authentication on their online accounts such as email and banking. They may want to make all their account passwords unique and long, and to freeze their credit files.

Some individuals may be particularly vulnerable. For example, people whose address was a secret, such as relocated victims of domestic violence, undercover police, judges, etc. They should contact Medibank urgently if they need relocation assistance.

Some foreign governments may be interested in the health information of people who have sought medical treatment in Australia (such as international students), which could create risks for people when crossing international borders. For example, a person who had sought treatment for drug addiction in Australia may face increased questioning by customs and immigration on their next trip home.

Host: As a nation - we've really had our eyes opened to the threat of hackers in the past few months. Do you think companies here have learned how to protect their data?

Dr Selby: Whilst many Australian companies and government agencies have started to lift their privacy and cyber security maturity levels, there is still a long way to go.

The new Privacy Act penalties are intended to motivate organisations to increase their investments in privacy and cyber security.

One of the areas where there is a lot of work to do is around data minimisation – Privcore often says to its clients “if you don’t need it, delete it”.

Dr John Selby interviewed by Channel 7 host, Gemma Acton.

Contact: media@privcore.com