Submission to2023-2030 Australian Cyber Security Strategy Discussion

This submission is based on personal experience. I was affected by the Medibank hack as a provider and the Latitude hack as an applicant for a financial product, to the best of my knowledge, decades ago. I am not a Cyber expert but wish to add my voice to those affected by these crimes, to express what might help security for a client of these large services.

Currently, many enterprises are allowed to collect and hold data which may be beyond their essential needs. It appears it is often held longer than necessary. And where retention is necessary the loss of this data indicates it is not held securely according to the goals aspired to in the *2023 Australian Cyber Security Discussion Paper.*

For me to access much of my own data held by financial institutions and the like 2 stage verification is commonly required. Surely for something like Medibank, a honey pot for hackers, something like this should be required of **ALL** staff to access personal data. Secondly all files stored in an enterprise's own or in third-party storage should be encrypted, so even when irregularly accessed and downloaded the file is useless to malevolent parties.

It seems evident to the layman that the scope of personal data being collected and held is excessive, and it is retained for a period way beyond necessary. To the best of my knowledge my dealings with Latitude or its acquisitions occurred decades ago and may have been no more than an application for credit not taken up by me. It seems a corporation's right to retain personal data and the facility to monetise it even internally exceeds the immediate need. Of course, It is necessary to collect information to correctly identify a

customer but why, once identity has been proven and how it was proven, is any further record of the primary document necessary?

Finally, if it is deemed that primary documents such as a copy of a driver's licence can be kept it is quite reasonable that this record be destroyed after a reasonably short time or at the termination of any arrangement between customer and holder of the personal information.

In summary, I suggest there be tighter controls on what can be collected, how it is stored and how long it can reasonably be stored.