# INTE1122: In Class Briefing Note (Assessment Task 2B)


## Sai Teja Bathula S4038096


## Semester 1 2024

## Data breaches affecting millions of Australians are on the rise.

The Latitude breach was one of Australia's biggest in recent history. UpGuard (2024) reports that Latitude Financial Services, had a ‘data breach that affected more than 14 million consumers in Australia and New Zealand’. A breach at Latitude resulted in unauthorized access to client personal data was caused due to stolen employee credentials. The data had been retained since 2005, prompting worries about keeping consumer details for longer than the statutory seven years.

To avoid future breaches, multi-factor authentication, frequent security upgrades, and prompt deletion procedures are required. Employees should get continual cybersecurity training to keep current on best practices and possible risks. These actions will greatly improve data security and avoid future intrusions. For example, after applying identical measures, Company XYZ reported a 70% reduction in attempted breaches in the first year, proving the efficacy of a complete security approach.

I recommend, Latitude Services should immediately deploy multi-factor authentication and undertake security assessments to improve its cybersecurity posture. To avoid data retention hazards, the organization should implement ‘data retention period of 2 years’ (Australian Government, 2023). ‘Improving staff awareness of cyber security issues and threats’ (OAIC 2023) is essential for maintaining knowledge and preparation in the face of possible attacks.

**References:**

1) UpGuard (2024) 13 Biggest Data Breaches in Australia, UpGuard website, accessed 30th May 2024. https://www.upguard.com/blog/biggest-data-breaches-australia

2) Australian Government (2022) Data retention obligations, Department of Home Affairs website, accessed 30th May 2024. https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/data-retention-obligations

3) Office of the Australian Information Commissioner (2023) Preventing data breaches: advice from the Australian Cyber Security Centre, OAIC website, accessed 30th May 2024. https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/preventing-preparing-for-and-responding-to-data-breaches/preventing-data-breaches-advice-from-the-australian-cyber-security-centre#:~:text=To%20mitigate%20data%20spills%20and%20breaches%20and%20other,mitigate%20the%20risk%20of%20brute-force%20attacks%20being%20successful