Just as we published our first quarter of 2023 update, the news hit about a breach at Latitude Financial Services. In terms of size, that makes it the second largest breach in Australia; just behind the 'Canva' data breach in 2019.

While Canva was the largest in size (# of users impacted), the 'severity' of what can be exploited to those affected certainly goes to Latitude, Optus and Medibank, which in many cases exposed the '100 points of identity'. But to their credit, Latitude provides an impressive level of transparency on the information compromised and advice to reduce the impact at their website.

Big Data = Big Target

What is one key lesson from the Latitude breach that we can use? Apparently "much of the data was stored from 2005"… really? 18 years of data!?!? We appreciate the Data Analytics team wanting lots of data to unlock business value, but at some point, you should reduce your risk by getting rid of old data. That data whose practical business value typically decreases as it gets older, but whose liability increases as single source of data that motivates criminals to steal because of its monetisable value!

It reminds us of the infamous quote from the notorious bank robber, Willie Sutton, who said he robbed banks 'because that's where the money is". While 'big data' can be valuable, it can also be valuable for all the wrong reasons too – from our experience, most 'data lakes' and similar data sources do a great job connecting ALL of the important data together. But because it's typically considered a 'back office' (not internet facing) system, it's left widely available to everyone in the organisation; then easily (and frequently) copied, and usually poorly tracked as to who accessed what or when.

Also analogous to Professional Services

The Willie Sutton quote also relates to the HWL Ebsworth attack this quarter. The Australian law firm interestingly filed and received an injunction from the NSW Supreme Court to legally 'prevent hackers from publishing any stolen data'. At first blush you'd wonder the sanity of spending the effort to get a legal injunction for a criminal who clearly isn't concerned about legalities. On reflection however, the potential ability to leverage the injunction to prevent media or other parties from reporting the details of the stolen data is an interesting angle worth considering if you find yourself in a similar position.

And, just how does this relate to the quote? If you have the confidential details of multiple people, clients or organisations; for example, most law firms, accountants, consultants, etc., then you will be a "Cyber Willie Sutton" target too. Being forewarned is forearmed – just let us know if you need independent and experienced help to clarify your top priorities to reduce your cyber risk!

Also 'where the money is'

This quarter saw the 'managed file transfer' software "MOVEit" get compromised, which impacts numerous international and local businesses who used this 'supply chain' software to exchange highly confidential or sensitive data. Locally, PwC and Medibank (as if they didn't have enough issues to deal with) were impacted by this breach, including EY and the OAIC as well.

Once again, 'it's where the money is'… If you use one of these types of confidential file transfer systems, just like reducing your reducing your big data as a big target, consider getting your users go through that system and remove all historical data that may come back to haunt you.

A "311" cyber hotline and Cyber Clinic??

We couldn't help notice a VERY INTERESTING concept titled "The Bold Plan to Create Cyber 311 Hotlines" published by Wired this quarter.

It's based on the premise that we're besieged by endless hacking campaigns that disproportionately burden under-resourced organisations like small businesses, charities, and community organisations; all whilst our State and Federal agencies are focused on the more serious threats to critical infrastructure.

The idea is that University 'clinics' could be the future of cyber defence at a smaller / local because "*Students are local, highly motivated, and able to provide a range of services pro bono for under-*

resourced organizations that otherwise couldn't afford them". The concept of a 'Cyber Poverty Line' for many organisations is real – and as noted in that article, threatens our entire cyber ecosystem.

Concurrently, we constantly hear about the lack of practical skills and short comings of cyber students in our education programs and their lack of hands-on experience. It would be an impressive Australian University or Tafe who stepped up to pilot a similar program like the University of Texas at Austin.

Password123 – the statistics are frightening

This quarter saw a wealth of statistics reinforcing the urgent need to improve how we all manage passwords and credentials to access important systems.

This year's Data Breach Investigations Report has nearly 1 million incidents in its data set, making it the most statistically relevant set of report data anywhere. Stolen credentials are the overwhelming leader in data breaches, being associated with nearly 45% of all data breaches.

To bring that home locally, the Latitude breach is blamed on a threat actor getting privileged credentials via a third-party vendor (have you assessed who has access to your systems and how they're managed?).

Sadly this quarter read that 78 percent of Australians use the same password across various accounts. And yet another shows that 83% of the most used passwords can be cracked in less than one second.

That data, when also combined with the fact that 74% of breaches involved 'the human element' (DBIR) says that if you only had $3 to spend on cyber in total, you might want to spend at least $1 of those on increasing your organisation's cyber awareness.

HOWEVER, it's not just about phishing emails, but designing and implementing sustainable behavioural change – recognising that change requires leadership commitment, that different personality types learn differently, and you should use techniques like operant conditioning and gamification as approaches to achieve sustainable cyber awareness.

Did NSW really cut funding for Cyber Security NSW?

With cyber threats escalating, is it really true that the NSW State government cut funding for its Cyber Agency in 2024? It's hard to understand the logic of that decision with breaches occurring on a weekly basis. Hopefully it's just politics, as one would expect changes when it was accused of not having a plan or authority, and indicating they'd respond several months after the accusation.

Quote of the Quarter - Cyber Insurance

Cybersecurity insurance isn't like other insurance such as car or health. "If you get in a crash, you know you will be covered. If you get breached you may not be covered because it's impossible to cover".

Thanks for investing the time to catch up with us this quarter. If you're not already, please 'follow us' on LinkedIn and/or Twitter, and feel free to send this to others (or have them subscribe here).

Kind regards,

TrustedImpact
PROTECTING DIGITAL

we're **independent** consultants – it's about **your** business and **your** success
with a **singular focus** – cyber security is all we do
leveraging **experienced** professionals – credentials, not checklists