2023 is coming into view as we finish off a tumultuous 2022. On the bright side, this year the world started to shake the shackles of Covid. The statistics show we fared relatively well against world statistics when it comes to fatalities – either absolute or per capita. As a friend of the firm noted "*all expectations were that it was time to return to normalcy – even if some elements of how we exist had changed forever'.*

The quarter that will define the next decade of cyber?

At the end of last quarter, the impact of the Optus breach was just unfolding. Soon after, a seemingly never-ending list of organisations announced a litany of data breaches – Woolies, Australian Clinical Labs, Telstra… So many, that apparently Australia ranked the 'worst' in the world for data breaches with 22 accounts hacked every minute.

Such a constant stream of data breaches can lead to data breach fatigue ('a stream of near-constant data beaches leaving consumers and organisations numb to security risks')? While the previously referenced article is a bit dated, it aptly notes that:

"At a time when data security needs to be taken more seriously, people are turning their heads away from the issue instead of working to stop the problem. It's essential that your organization recognize breach fatigue in its own security strategies and in its employees, and work to reverse this complacency to protect the business."

One way to help with your Board and Exec's is to be armed with a few of the local statistics. For example, one survey notes that one tenth of Optus customers have churned after the breach and around half were still considering changing providers. What is 10% (to 50%) of your organisation's revenue look like – particularly if that revenue is recurring? Furthermore, Optus flagged a $140 million cost for the breach. While Medibank's estimates are much lower at $25-35 million (likely due to not paying for replacement identity documents), $1.8 billion was wiped from its' market capitalisation since the breach.

The Optus breach teaches us to be concerned about poorly created or secured 'Application Program Interfaces' while the Medibank breach tells us that turning on Multi-Factor Authentication for EVERYTHING is essential. Simply put, the cost of those measures (or getting help to assess those things) would be a tiny fraction of the cost of the breach.

Lessons learned?

What other lessons can be used to your advantage so that your organisation isn't the next cab off the 'hacked' rank? It's clear that our old mantra 'In the Digital Age, a security breach is inevitable – but becoming a headline doesn't need to be' rings true.

First, having a clear, well thought through position PRIOR to an incident pays off. Details such as who should be the 'face of the organisation' is an interesting topic when comparing Optus to Medibank. Albeit, the unfortunate 'trainwreck' of an interview for Optus was a lesson in preparation at all levels and not just the Information Technology team. Remember that it's not just the strategy or plan, but about practicing it – we have a unique and valuable simulation approach if you'd like to explore how your organisation can better prepare for the inevitable cyber incident.

Hard to fathom and definitely 'salt in the wound', we feel obligated to note the audacity of Medibank's deplorable $7.3 million executive bonus payments approved in November. It highlights the simplicity of one - often overlooked - change you can make to significantly improve the security of your organisation. That is simply aligning your executive KPI's with the confidentiality, integrity and availability of your technology and data assets. Perhaps Medibank's investor threats of executive pay 'clawbacks' and class action lawsuits will reinforce the importance that simple, yet powerful approach. The Medibank Chair's comment "safeguarding our customers' data is a responsibility we take very seriously" becomes awfully disingenuous when paying millions of dollars in performance bonuses only weeks after losing the private data of nearly 10 million current and past customers.

Clare O'Neil – kicking goals

We continue to be impressed by the Minister for Cyber Security, Claire O'Neil, who is following through on her September promise to update cyber policy reforms. In fact, it's fair to say that she's made more progress in the past few months, than previous governments made in years. Her speech to the National Press Club in December is eloquent and impressive. She hit the nail on the head when she said:

> *The truth is, **we are unnecessarily vulnerable**. We did not do the work nationally over the last decade to help us prepare for this challenge. Prime Minister Morrison's decision to abolish the Cyber Security Ministry when he came to office was a shocker.*

There's also been impressive progress made to coordinate with 36 other countries to stem the impact of ransomware. In particular, The Department of Home Affairs will convene and host an International Counter Ransomware Task Force as part of the United States-led Counter Ransomware Initiative. And we're proud to see Australia playing a leading told as the coordinator of the Task Force.

New Ramifications

The 'teeth' intended to motivate those organisations that are the custodians of our personal and confidential data is a bill that was passed in November that raises the penalty for businesses that suffer repeated or major data breaches. In short, the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 will increase the civil penalty from $2.2 million to whatever is the most of:

1. $50 million;
2. 30 per cent of adjusted turnover for the period;
3. three times the financial gain from the misuse of data in the case of outstandingly shocking breaches.

While we agree there needs better definition around how and when penalties are applied, the implication that it will 'dampen innovation and create an environment that hinders consumers and organisations making lawful and ethical use of data' is dubious. A bit of 'secure by design' thinking should be a fundamental part of any innovation effort. This is a positive step to help protect both; consumers, and businesses alike. Simply stated, a more resilient country will be a more prosperous country.

However, what appears to be missing was painfully illustrated in the recent report: "The Commonwealth Cyber Security Posture in 2022". Quietly released just a few weeks ago, this report uncovers that a meagre 11% of Commonwealth organisations have reached a Maturity Level 2 of the Essential Eight. Furthermore, over half (51%) of the 185 entities covered in that report have not exercised an Incident Response Plan within the last three years (or more).

At the risk of being hypocritical, we suggest the Government should create similar penalties to be consistently applied to all organisations, including Government organisations – many of which capture as much, if not more, sensitive personal data than Optus or Medibank.

———

Thanks for investing the time to catch up with us this quarter. May the New Year be full of peace, joy and good health! 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