The first quarter review March 2023

This quarter we saw the US shooting ‘objects out of the sky’ and devastating earthquakes in Turkey and Syria. Silicon Valley Bank just fell over (the 16th largest bank in the US and 2nd largest failure in US history). Soon after, Signature Bank closed; making that the 3rd largest bank failure in US history. Next Credit Suisse added to the tension… fortunately they received a A$81 billion lifeline!

Before that happened, the general view of the economy was that this year would be challenged by slow economic growth and rising interest rates. The five year graph of interest rates in Australia is daunting.

While the worldwide economy appears to be braking hard, the opposite continues in cyber. We’ve been foretelling skill shortages in the cyber industry for some time. But it’s just starting to become real. Skilled or experienced cyber pros are hard to find; so, expect salaries and costs to increase, and availability to decrease. That ‘last minute penetration test before we go live’ will require more advanced planning.

Also, while self-serving, it will also be prudent to look to organisations like Trusted**Impact**, to compliment your organisation’s capability as the ability to hire your own cyber staff will be difficult. There also appear to be a growing number of new cyber graduates, so if you want to try to build your own team, expect to invest heavily into skill development.

The bloody aftermath of Optus and Medibank.

The Financial Review noted in the start of the quarter that The Optus brand suffered a $1.2 billion blow after last year’s cyberattack, and when it happened, $1.6 billion was wiped from Medibank’s market value. Those are some big numbers to help your call for investment in proactive cyber protection! Watch this space however, this quarter saw three law firms joining forces on a Medibank Class Action law suit.

Even with that kind of eye watering data, it’s astonishing to read recent survey results from Netskope that found OVER HALF of Australian organisations admit they haven’t invested enough in cybersecurity and that nearly ONE in FIVE believing cyber was a not a priority.

Including a raft of legislation…

Mandatory reporting of information security incidents came into effect for 11 critical infrastructure sectors last year after changes to ‘Security of Critical Infrastructure’ (SoCI) laws. This quarter it was reported that 47 reports were provided in the first nine months of the mandatory reporting regime.

Following that, in Feb, the Critical Infrastructure Risk Management Program (CIRMP) Rules commenced. If you have any critical infrastructure ‘assets’ you need to be across the detail. In short, it requires ‘responsible entities’ to become compliant with ONE OF FIVE cyber frameworks by August 2024. We’ve helped hundreds of organisations with those frameworks – so drop us a note if you want some practical insight or help to understand what that might mean for your organisation. Just for that program alone, The Office for Impact Analysis estimates that it will cost A$11.5 billion over the first 10 years to comply with those requirements.

But that’s just the start when the Minister for Cyber also “slammed the former Government’s cyber security laws as “useless and flawed” after finding themselves unable to effectively respond to the Optus and Medibank incidents”. As a result of the “bloody useless, like not worth the ink printed on the paper” laws, a new ‘Cyber Agency’ will be created to “provide some strategy and structure and spine to the work being done across government”. It will all be a part of a new Cyber Strategy, which is currently seeking submissions until mid April 2023.

Hopefully that Strategy will not just add another framework to align with. The issue is easily illustrated with the CIRMP Rules which requires one to aligned with ONE of FIVE different frameworks. We have plenty of frameworks and most certainly don’t need more clarification as Andy Penn suggested here.

We think it’s about making organisations (public and private) accountable to identify and manage their risks. Don’t forget that in 2022 a meagre 11% of Commonwealth organisations reached a Maturity Level 2 in the Essential Eight.

We also agree with InnovationAus.com’s article that “The obligations of directors are already clear; making them explicit or establishing external frameworks for compliance monitoring will only add additional costs without improving standards.”

Will the cyber insurance industry be viable?

In Q3 we highlighted the disconcerting trends in cyber insurance. That was further reinforced this quarter when Zurich Insurance Group's CEO signalled that cybercrime will become 'uninsurable'.

It was looking pretty gloomy until the US Biden administration just released its Cybersecurity Strategy. Details are sketchy, but the new US Cybersecurity Strategy says it will "explore how the government can stabilize insurance markets against catastrophic risk to drive better cybersecurity practices and to provide market certainty when catastrophic events do occur." Yet Washington Post's analysis of the strategy noted; it's prompted plenty of debate around sub topics like whether it would help steady the cyber insurance industry, or invite organizations to take greater risks.

LastStraw for LastPass…

Password reuse is a considerable problem. One 'simple' answer is a password manager which can help manage the multitude of passwords/passphrases that we need to manage. That is, unless your password manager is breached – either through you having your details compromised, or via the password manager itself getting compromised.

LastPass is one password manager that has a litany of issues in the last few years – summarised here - which highlights a long systemic trail of concerns. In short, it would be prudent to shift to another password manager (there are plenty of reviews for top programs).

But don't stop there! The 'double blind' method sounds complex, but is both elegant and powerful to minimise the risk of someone gaining access to 'any' password manager. In short (and described very well in this video), before entering that 'complex password' generated by the password manager into the website – simply append it with a 4 (or more) 'hidden code' that only you know (don't add it to the password manager). That way, the bad guys might get the generated complex password, they won't have your appended code that only you know. An elegant approach that, much to our surprise, many in cyber aren't aware of.

Significant Salient Statistics…

Each quarter we trip across a wealth of statistics. When used sparingly and in the right context, they can often improve a conversation with your executives and peers.

This quarter, we learned from McGrathNicol that FOUR in FIVE (79%) of Australian businesses chose to PAY a ransomware ransom of over $1 million. Worse; "the average amount that businesses would be willing to pay however, is higher".

With those numbers it's no wonder that mimecast estimates that cybercrime will cost the world $8 trillion this year. In terms of Gross Domestic Product (GDP) that would be THIRD largest country in the world, just behind the US and China or more than four times larger than Australia's GDP.

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