The second quarter update
June 2021

The air of optimism from last quarter was dampened when Victoria announced its fourth lockdown in late May. Just in the past few days, lockdowns have now been called in several other areas around the country. Australia's apparent aspiration to eradicate the virus seems futile, and National vaccination rates are far from impressive at less than 5% of the population.

There's mixed results around the globe too. McKinsey coined it 'today's pandemic paradox': global growth is rebounding, even as the virus's spread persists. While global public health remains in a fragile state, industrial output has increased, with big gains in manufacturing, services, and trade. Furthermore, many indicators point to strong growth momentum for China and the US, although observers are certainly pondering what will happen with inflation. Locally, the ASX All Ords have grown about 25% since this same time, last year.

It therefore strikes us that there are three important take-aways from the current state of affiars:

1. **Uncertainty and variability will be with us for some time still** – cyber criminals prey on uncertainty, variability and fear. So, if you're not actively raising your organisation's cyber awareness, you really should be. Remember that it's not just about training, but instilling behaviour change – we have proven approaches if you'd like help with cyber behaviour change.
2. **Digital channels to customers and with suppliers are here to stay**. The good news is that 66% of the world's population is now online – the ability to reach the users across the globe has never been easier. However, the bad news is that some portion of that VERY large population of 5.2 Billion users may try to exploit your digital channel. If that portion were just 1 out of 100, that's more than TWICE our entire population in Australia. Protect your digital channels by testing them. Testing has been a fulltime endeavour for us over 14 years – over that time, we've seen programming vulnerabilities reduce, but CONFIGURATION issues skyrocket. CVS, the American pharmacy learned that lesson this quarter when it lost over a billion records thanks to a cloud configuration issue. Eversource Energy learned the same lesson when a 'cloud data storage folder' was misconfigured so that anyone could access its contents. So, don't JUST test, but assess your cloud's CONFIGURATION. Either use the CIS Benchmarks, or ask us to do it – we can almost guarantee you've got configuration issues.
3. **It's all about Resilience**. Ransomware is rampant and we need to start thinking about the concepts of immutable backup. Channel Nine's incident last quarter also reinforced the need to be able to restore bespoke applications as well as just recovering data. Have you thought through the steps, roles and responsibilities of an incident? A professional footy team has a playbook, and they practice those plays to ensure they can execute to a tee. If you have a plan, have you ever practiced it? If not, check out our Trusted**Response** simulation platform.

Ransomware = Terrorism.

As Ars Technica aptly noted; "this has to be at least the fifth consecutive 'Year of Ransomware'". In other words, each year surpasses the last's year in terms of expectations and growth. That's supported by the data that shows that the average ransom payment (of US$233,817) has increased 31% from last year alone.

The 'silver lining' from last quarter's Colonial pipeline incident, is that the U.S. Department of Justice have now given ransomware hacks similar priority as terrorism. That's significant when you consider the average spend in the US on counterterrorism (2002 to 2017) was "more than Russia, India and South Korea spent on defence in 2017 combined". And if there's one clear thing that came from 9/11, it was the US Government's ability to 'follow the money', which is how apparently the majority of the $4.4 million ransom was recovered. Here's hoping this will stem the exponential growth of this risk!

That said, additional news came to light about the Colonial ransomware, which demonstrates that it's still about "the basics" when it comes to protecting most organisations. While "Operational Technology" has long been seen as the "Achilles' heel" of most critical infrastructure providers, apparently the ransomware actually did not impact any of the infrastructure systems. EVEN WORSE, instead of it being the savant skills of an elite hacker, we learned that it was simply a dormant VPN account with no Multifactor Authentication (MFA) protection.

So, what can we learn from this and apply locally? Your organisation probably has a strict 'policy' about passwords and one that states that all accounts (particularly privileged) should be removed. BUT have you ever actually analysed your Active Directory for dormant accounts, or bad passwords? We do a lot of that type of work, and you'd be astonished just how misaligned policy is from reality. Do you actually know if you have any old, dormant (privileged) accounts? Also, if you do not have MFA turned on for ANY and ALL internet-facing access (or cloud services), do it, and do it now.

Cyber Guide for Boards of Directors

The World Economic Forum can be a good source of contemporary cyber information. This quarter they reinforced that Boards of directors need to play a more active role in protecting their organization from the growing threat of cyber risks, and aptly referred to a PWC Survey which found that few fully understand the risks. The study notes six principles that can be applied across industries and geographies. While these principles won't sound incredibly novel to most hardened cyber professionals, they are well aligned to the Board level and provide good contextual advice for Australian Boards too.

Essential 8 - New & Mandatory?

CSO Australia just tipped that the Essential Eight will (may?) be mandatory across 98 noncorporate Commonwealth entities. That said, it wasn't clear whether it's actually become mandatory, or that the Government is 'preparing to act'. Just preparing? The majority of all contemporary security frameworks (NIST, ISO, PCI, etc), at a granular level, have controls numbering in the hundreds yet for apparently some organisations (which store vast amounts of incredibly sensitive information on all Australians) they're 'preparing' to consider implementing eight controls? If we're really tired of having data breaches, or want to take ransomware seriously, then eight controls doesn't seem that draconian.

In parallel, the ACSC has also tipped a '**NEW**' updated version of the Essential Eight with added clarity and recognition of maturity levels. Having the two happen in July would be a positive step forward. Watch this space or sign up for ACSC Alerts here.

While the Essential Eight are a great start, they're primarily focused only on 'technical controls'. The statistics show that a majority of data breaches start with a phishing attack, so don't forget that one of your biggest risks are those staff who are naïve to the risk of social engineering and phishing emails. Therefore, if you only had 'two dollars' to spend on security, awareness should probably be one of them. We've got some great awareness platform partners and can help so that you don't need to reinvent the wheel.

_____

Thanks for being part of our community. If you're not already, please consider 'following us' on LinkedIn and/or Twitter, and don't hesitate 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