The second quarter review
June 2022

It's hard to believe we're half way through 2022! This quarter the economy has taken a hit for the worse; inflation is escalating, which is fuelled by continued supply chain shortages and spiking energy prices. Furthermore, the RBA has just released the first 'back to back interest rate hike' in more than 12 years.

One thing is clear - times will be tight. So keeping an eye on your cybersecurity spend will be important. That said, don't be foolish and take (cyber) risks inadvertently or unconsciously without considering the likelihood and consequence of an incident to your organisation – particularly in a world where having a 'digital' presence may be the difference between business success and failure.

We think we're pretty good at identifying the unique risks to an organisation, and pride ourselves in helping organisations with a 'health check' or 'maturity assessment' to tease out TOP or important risks to mitigate, rather than giving you the 'lazy auditor's' exhaustive list of hundreds of controls you have to implement. With this tight business environment, it might be time to take stock of your top priority cyber risks to mitigate – just drop us a note here if you'd like to understand what that might look like.

Ransomware creates an 'official state of emergency'.

At the start of the Russian invasion of Ukraine there were lots of cyber professionals on edge, suggesting the next generation of WannaCry, Petya and Not-Petya would rage across the global digital landscape. Authorities were beating the drums suggesting that Australian organisations should urgently adopt an enhanced cyber security posture. Fortunately, at least so far, there hasn't been much devastation seen in that space so far.

However, one area that HAS 'rung true' to all previous warnings is the pervasiveness and devastating impact of ransomware by criminal groups. This quarter the Country of Costa Rica officially declared an official state of emergency due to a massive ransomware attack that it continues to try to recover from – this is the first time a country has done this in response to cyber attacks. Frightening to first read about, but even more frightening when one delves into the detail to read what one of the 'first responders' noted that "There were no backups whatsoever". Really?

Therefore, it's time again to check, double check, and triple check that your Disaster Recovery and Back Up strategies are in place to recover from this (potentially devastating) threat. Remember that Channel Nine reinforced the point that it's not just about recovering data, but bespoke systems that might not be easily recreated. Sound advice and practical steps from the ACSC can be found here.

Also, don't forget that the threat can also come from all directions. For example, criminals are going direct to your employees to ask them to unleash malware for a cut of the ransom. Therefore, your strategies should involve the ability to recover, even if an 'insider' has visibility or access to your systems.

Simply paying the ransom may not be the answer either. This study by Sophos, found that nearly half (46%) of organisations paid a ransom to get data back, but only 4% that paid the ransom got all their data back. On average, those who paid still lost 40% of their data even after paying the ransom.

Therefore, given the significant business impact that ransomware is having in virtually every sector of our economy, consider engaging someone independent (and experienced) from your team (or supplier) to double check that your recovery strategies are practical and proven - not just theoretical. We can help with that too if you're interested – if so, just drop us a note here.

Finally, a dedicated – DIVERSE – Minister for Cyber!

Last quarter, we mentioned that Anthony Albanese signalled his position with great clarity on the sizable risk that Australia faces with cyber security. Well, this quarter we were delighted to see the appointment of a dedicated Minister for Cyber Security.

This appointment is important for TWO distinctly different reasons. The first reason resonated when Albanese observed that because of the size and importance of the problem, "Cyber security needs to be someone's day job, not the last item on another Minister's to do list." We often talk about how cyber is a 'leadership challenge' and not simply an IT problem. It's about time we've elevated this issue to the right level in Government.

The second, perhaps even more important reason is the fact that the appointment clearly addresses the need for our industry to improve its diversity (of all types). The appointment of Clare O'Neil, as Minister for Cyber Security sends a long overdue message that there is opportunity for more women in cyber to fill the most senior and prominent positions in the industry. Irrespective of your political persuasion, achieving greater diversity in cyber is important and this move should be applauded and supported by all corners of our industry.

If it's true there… it's true here too.

The Washington Post published a thought provoking article from a survey that implies that the United States is **'just as vulnerable – or even more vulnerable – to cyber attacks' then it was five years ago**! While the article reflects the US environment, it would be exactly the same situation in Australia.

We can corroborate that progress has been made. However, what is exacerbating the issue is our rapid adoption of technology, the pace of digital transformation, and our insatiable appetite to connect devices of all types (IoT) without recognising the role of, or simply prioritising security. So, what's the point? Elevated cyber threats are the 'new normal' – it's probably time to invest in a thoughtful, program of risk reduction that's tailored to your organisation; not just by purchasing 'silver bullet' technology. Drop us a note if you think it's time to do a holistic review and put a reasonable plan of risk reduction into place.

SoCI – are you really ready?

Last quarter we highlighted the momentum behind Security of Critical Infrastructure (SoCI) Act. It designates new industries as critical infrastructure, and expands compliance obligations for reporting and risk management. The act is enforced by a range of civil penalties, including imprisonment.

However, complying requires disparate functional groups from Operations to IT to work seamlessly together – a historical morass for most traditional utilities in Electricity, Gas and Water. Because of this we've partnered with GMDR Group, a specialist Utilities Operations Consultancy to help those types of organisations understand and successfully respond to this onerous, new requirement. Drop us a note here if you fall into one of those categories, or want to understand more?

Parting thoughts

This quarter, the US Cyber and Infrastructure Security Agency released findings from 112 Risk and Vulnerability Assessments (RVAs) across multiple sectors in 2021. The infographic results are insightful. At a high level, the obvious culprit? 'Valid Accounts'. Therefore, if you're not using MFA for EVERYTHING external and for EVERYONE in the organisation, you should reconsider that position.

____

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