The third quarter update
September 2021

The COVID Delta variant took off in Australia this quarter, and as a result most of Australia has been hunkered down since. We finish this quarter mostly in lockdown as we push for more vaccinations in the hope that we can begin to open up as summer approaches. It's definitely been a challenging two years for everyone – keep strong and keep safe – this too will pass in time! We're all feeling a bit worn down living in Bill Murray's 'Groundhog Day' (don't tell us you can't relate to this great YouTube clip!).

A cybercrime report every EIGHT minutes.

Unfortunately the old saying "crime doesn't pay" doesn't seem to be true with cyber. This was shown in the latest stats this quarter from the Australian Cyber Security Centre's (ACSC's) Cyber Threat Report 2020-21, showing Australian cybercrime reports are up 13% (or now one report every 8 minutes – up from every 10 minutes last year). The fact that there's one page of valuable cybercrime statistics – all headed in the wrong direction – versus two pages of 'what the ACSC has done' shows that there is still a lot more needed to begin to stem the tide.

Ransomware the highest threat.

No contemporary discussion on cyber would be complete without a focus on Ransomware. While the numbers show that fraud is the most common category of cybercrime, the ACSC now assesses ransomware as the highest threat.

The threat can also come from all directions. For example, apparently now criminals are actually going direct to your employees to ask them to unleash malware for a cut of the ransom. Also, whether or not you believe it's right to pay a ransom, you should realise that many ransomware programs actually end up corrupting the data along the way. So, even if you do pay, there's no guarantee you will get your information or systems back.

Therefore, it's clearly time to check, double check, and triple check your Disaster Recovery and Back Up programs to ensure you can recover from this (potentially devastating) threat.

The principals of 'immutable data storage' become an important term to understand – a pretty good explanation YouTube (28 mins) might be worth watching if you want some of the fundamentals to consider (thanks for the link Ben!).

To help even more, the UK Cyber Security Centre (NCSC) released a helpful "Ransomware: What board members should know and what they should be asking their technical experts".

Why should the Board be asking these questions?? ICT Legal Consulting offered a sound answer:

> *The fact remains that, the current requirements under the Corporations Act already render directors liable for cyber security… directors can also become* ***personally liable*** *as a result of breaching director duties that caused the company to suffer loss.*
>
> *So, failure to identify the risk of ransomware (****due diligence****), and failure to address the risk of ransomware* ***(due care) can already render a company director liable under the Corporations Act.***

It might be worth sharing this article with your board...

One final work on ransomware is to remember what we learned from Channel Nine last quarter – that it's not just about data, but critical systems (often termed "Operational Technology") which, if compromised, can also bring the business to a halt.

Why not here… did we forget?

In August, the US demonstrated some impressive Government / Business collaboration when President Biden hosted a cyber security summit with CEO's in industry sectors ranging from Technology to Insurance. Impressively, Apple promised a program devoted to making security improvements, Google committed $10 Billion to strengthen cyber security, and Microsoft committed $20 Billion (among many other things).

Reading that, we couldn't help but remember that a key plank in the 2016 Federal Cyber Security Strategy was to develop a 'National Cyber Partnership' where;

> *"Together, the Australian Government and business leaders will jointly drive Australia's cyber security, setting the strategic agenda through annual Cyber Security meetings. Hosted by the Prime Minister and comprising leaders from business and the research community, the meetings will align the key initiatives in this Strategy and tackle emerging cyber security issues. A Minister Assisting the Prime Minister on cyber security will also underpin this effort."*

Prime Minster? Minister Assisting the Prime Minister? Outside of a small Advisory Committee apparently established late last year, it seems Australia well and truly lost sight of the potential for Government and Australian Businesses to collaborate on the cyber risks that we all face together. (as an aside, the Government/Business relationship sounds considerably more antagonistic these days, as Canberra pushes 'Emergency Laws' to give itself increased powers if it deems appropriate).

While it can be difficult to influence the political agenda, try to not let a lack of leadership happen in your organisation! If we reflect across a 15 years of cyber security consulting to more than 300 organisations, the most significant difference between those who are well secured and those who are not, is a leadership group that recognises the importance of cyber security.

To be clear, they don't need to be the experts – but simply to set the appropriate tone and make it part of the organisation's agenda and ongoing conversation.

And don't just hope the executive group will get it either. If you're in a security role, that means frequent, formal, and structured interactions. In particular, providing them with the 'narrative' so they can support you with the business challenge of cyber.

Ten years ago, the Chief Security Officer (CSO) was often recognised as the sole person 'responsible' to protect the organisation – we know now, just how naïve and short sighted that view was. Successful and effective CSO's are enablers who can successfully engage the most junior staff to the most senior.

The 'top 30' is worth checking for your organisation

In July the US, UK and AUS released a joint cybersecurity advisory on the top Common Vulnerabilities and Exposures routinely exploited by cyber actors in 2020 and those vulnerabilities being widely exploited thus far in 2021. There's a range of issues relating to Citrix, Fortinet, Atlassian, Microsoft and other vendor software. It's worth double checking to make sure you've applied the appropriate patches!

This quarter marks our **FIFTEENTH birthday**! We couldn't have lasted this long without some REALLY GREAT consultants helping some REALLY GREAT clients every step along the way. Sincere thanks goes to everyone involved, including you, our broader 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