The third quarter update
September 2022

2022 is moving fast and it's hard to believe we're nearly into the last quarter of the year. Things aren't looking particularly rosy as we reflect on this quarter's insights. The war in Ukraine continues, inflation rates are at a 10 year high; El Nina is causing havoc with our weather, and sadly we lost the second longest serving Monarch in history, when Queen Elizabeth II passed away this month.

Breaking news… likely to change the 'tone' of the cyber discussion

Better insight will be gained in the following days and weeks about what really happened with the Optus data breach that is 'hard to fathom'. Highly sensitive personal data on more than ONE THIRD of our entire population, and nearly 3 million individuals with most of the data needed to pass a "100 point of identification" check. There's now an offer for free credit monitoring by Equifax… does anyone else see the awkward irony in that? The key question is 'who else' stores 100 points of identification so we can stop the bad actors from getting that information too!

Ongoing updates on the breach are here. Who knows whether the 'ransom' threats are real at this point, but it adds a practical twist worth making sure that it is considered in your cyber incident response plan (if you don't have one, or want to simulate that plan before it is real, drop us a note here).

It also remains to be proven, but we had to wonder whether this was actually foretold by the US Cyber Agency who, back in **June** warned that Chinese-backed hackers had breached a number of sensitive victims worldwide "including major telecommunications companies" rather than just a few days ago?

Straight on the heels of the Optus breach, the new Cybersecurity Minister, Clare O'Neil announced she will reveal new cyber policy reforms forcing businesses to be more responsive to customer exposures. She also showed impressive clarity when interviewed on the Optus breach recently – it's refreshing to hear someone in authority question the 'age old excuse' that a hack was the work of a 'sophisticated nation state'. It's an impressive conversation worth watching here.

Perhaps these revelations will also stem the disconcerting discussion around 'safe harbours' for Australian Directors accused of violating their legal obligations to prevent cybersecurity breaches. To be clear, and with all due respect to Mr Gonski, cyber is a business and leadership challenge - not some unfathomable technical wizardry that can't be understood by leaders of an organisation.

Any Director worthy of being on a listed-company board, should be able to tease out the key risks of an organisation (whether they be financial, operational or cyber); to set the right tone and priorities to adequately protect the organisation's most valuable assets; to question whether adequate resources are employed to mitigate those risks, and to strive for overall resilience. In fact, if you would like help, we do it all the time – just drop us a note. For example, a recent World Economic Forum (WEF) paper on "Advancing Organizational Cyber Resilience" presents six sound principles (24 sub components) that any Board member can understand.

Either way, perhaps the best thing (so far) from the Optus breach is the unattributed quote that 'People pretend data is gold — it isn't; it's uranium – super useful if used correctly and incredibly dangerous to just have laying about." Albeit, that quote is slightly behind Cory Doctorow's similar comment (in 2008) that "Personal data is as hot as nuclear waste… we should treat it with the same care and respect as weapons-grade plutonium: it's dangerous, long lasting and once it has leaked there's no getting it back"!

Ransomware… STILL!!

In August, the Australian Cyber Security Centre (ACSC) reinforced that ransomware continues to be the #1 threat to Australian individuals and businesses. There's lots of sound advice on how to protect yourself from ransomware here.

The first step is to get your team focused on that advice. But DON'T STOP there – if the survival of your business is important, get someone INDEPENDENT to validate your protection against ransomware is effective. It's a real threat – the Australian Competition and Consumer Commission's (ACCC's) found that scammers drained $2 billion from Australians last year, with ransomware and malware scams increasing nearly 1,500%! While providing independent advice is our business model, with those kinds of statistics, don't just let someone say 'she'll be right mate' - get it checked, if not double checked, by someone experienced and independent.

Concerning Cyber Insurance Trends

If you're thinking that insurance will cover your cyber (or ransomware) losses, be very careful and read the small print. A recent Australian lawsuit in August over ransomware insurance cover ruled the victim can **NOT** claim costs it incurred in the clean-up and recovery such as forensics, incident response and replacement hardware.

We also just learned that insurer, Lloyds is looking to EXCLUDE "Catastrophic Nation-Backed Cyberattacks From Insurance Coverage". This sets an interesting precedent that if the government attributes a cyber attack to a nation state, then the victims of the attack may not be covered by their insurance for losses incurred. Furthermore, if the government declines to attribute the attack to a nation state, the burden of 'proof' falls to the insurer, who is financially motivated to attribute the attack to a nation state. There's more insight and information here and here (thanks Kim!).

Cyber better linked to 'patient outcomes'

We're fortunate to do a lot of work in the healthcare sector, and it's all about "patient outcomes". Often, if one can demonstrate how to improve patient outcomes, most medical professionals will support the approach whole heartedly.

Historically, cybersecurity was viewed as NOT relating to patient outcomes and just about protecting 'confidential patient records'. But as the lines between medical technology and patient outcomes become more and more blurred, the importance of cyber to patient outcomes is clear.

So, if you're in the sector and need support to improve your cybersecurity posture, you should get a copy of a recent study from a highly regarded cyber research centre (Ponemon Institute) that you can share with your healthcare Executives and Board members. Although the data was 'American-centric' it's relevant in Australia. In summary, the study "interviewed more than 600 information technology professionals across more than 100 healthcare facilities. The findings are some of the most concrete evidence to date that the steady drumbeat of hackers attacking American medical centers leads to patients' receiving worse care and being more likely to die."

Other trends and insights

We've always advised the value of using Multi Factor Authentication (MFA) for EVERYTHING. As we (finally) begin adopting MFA, be wary of a new technique called 'MFA Fatigue' which is being used by hackers to trick people to give them authorisation. There's a good video example in that link. Also, make sure this is covered in your Cybersecurity Awareness Programs. If you don't have one, we can help you build one focused on not just phishing, but Behaviour Change!

For more cyber insight, Darren Arnott (our Practice Lead – Technical Consulting) has been prolific on LinkedIn – check out his posts here, here, here and here. They're quick and insightful!

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