When reflecting on this quarter's events, we found it interesting that this year is poised to be one of significant political change. 79 countries, representing over half of the world's population are expected to conduct national elections.

But while political change is on the horizon, one thing that will likely NOT change, is the continued pace and growth of cyber incidents. While many 'traditional' risks often maintain a degree of constancy over time, cyber is not the case – the likelihood is increasing as explained well in this Harvard Business Review article which is worth a quick read.

This was reinforced in February, when the Office of Australian Information Commissioner (OAIC), released its Q4 2023 statistics, which found that data breach notifications were up 19%. We also consistently talk about the need for 'behaviour change' when raising cyber awareness in organisations – this was also highlighted when breaches due to 'human error' jumped a whopping 36% as well.

In fact, the topic of needing a cyber 'behaviour change' was also the number one item on the Forbes "Tech Council's" list of "19 Common Cybersecurity Myths And Misconceptions". As noted, "*The myth is that cybersecurity training is going to help everyone get smarter about security… What we really need are tools that connect cybersecurity risk to specific activities as a way to help people practice better security hygiene*". In other words, not just 'phishing' staff or making them take online courses, but applying behaviour change techniques such as 'operant conditioning' (among others). It should be a cornerstone of any sound cyber improvement program – just let us know (here) if you want other ideas on how to improve your cyber awareness program so it isn't a burden and actually reduces your risk.

There were a few other worthy 'misconceptions' from the Forbes list – for example;

- "Cloud platform providers fully cover cybersecurity needs" (remember the adage, there is no cloud – it's just somebody else's computer?), and
- "The misguided believe that cybersecurity is an unnecessary financial burden rather than a strategic investment".

The other misconceptions are a good list to consider when thinking about your cyber program.

And while we're on the topic of cyber as a strategic investment, McKinsey also published a good note on "New-business building: six cybersecurity and digital beliefs that can create risk". We loved the comment that "Nobody ever created a unicorn by having another meeting". They also highlight several 'principles to illuminate the way forward' which are worth highlighting; notably,

- "If a concept merits investment, it is worth an Executive's time to consider and mitigate risks", and
- "Forward-looking 'New-Cos' see cybersecurity as a core element of business architecture".

Interweaving cybersecurity into an organisation's business strategy is fundamental in today's digital age. We particularly liked the quote:

"…*while business leaders are renowned for their ability to get things done, there is a flip side to the value creation gene. In the rush to market, it is easy to forget that the world's most successful companies have often withstood early threats to their viability. Indeed, our experience shows that business leaders who build resilience into their strategies are most likely to create winning propositions.*"

In fact, that issue came home to roost this quarter for Inspiring Vacations, one of the "2023 AFR Fast Starter's". The company had a stated goal of building a billion-dollar company by 2025, yet in February a cybersecurity researcher found a non-password protected database (aka 'open S3 data bucket') that exposed 112,000 records totalling 26.8 gigabytes of private and confidential information such as traveller passport photo's and numbers, CV's of applicants, etc.

While their website spruiks their awards for business growth, we found it disappointing they don't appear to mention any commitment to protect their customer's highly confidential data in their Vision or Promise! We all make mistakes, but we also think one should owe up to those mistakes if or when they happen.

MOAB: the 'Mother of all [Data] Breaches'!?!

In late January a 'Twelve Terabyte Treasure Trove' of 26 BILLION records was uncovered with usernames and passwords. Prior to the discovery of this, the previously largest recorded leak contained just 3.2 billion records. It's often hard to conceptualise those kinds of numbers, but simply stated that's 1000 times the ENTIRE POPULATION of Australia!

So, what does that really mean for you (or others in your organisation)? Well, if you (or they) have EVER reused your/their company password(s) in other websites like LinkedIn or Canva (or the other 18 sites listed here, which each have over 100 million records leaked), then it's highly likely your password is known to bad actors. You can also be pretty sure that those bad actors will then try to use those passwords to gain access to other important websites that you or your company have or use.

So, it's (past) time to use a password manager and stop making excuses that it's too hard! The other fundamental thing is to ensure that you have turned on Multi-Factor-Authentication for EVERYTHING you access on the internet – do it and do it now!

In fact, just the other day, we had a conversation with a membership-based organisation who said "our members don't like the inconvenience of using complex passwords, so we use their birth date as the default password"… Honestly!?! If you oversee an application that people access via the internet to transact or get access to important data, it's high time you start 'doing the right thing' by your users and not expose them to the risks of credential stuffing that was highlighted by the ABC in January.

But it won't happen to us, right?

Late last year, 23andMe a company that offers a "DNA Ancestry Test Kit" announced a data breach that went from impacting 14,000 users to 6.9 million users. Now with more than 30 lawsuits from victims of its massive data breach, 23andMe is now trying to deflect the blame to the victims themselves in an attempt to absolve itself from any responsibility and stating that "*users negligently recycled and failed to update their passwords following… past security incidents, which are unrelated to 23andMe*."

Yes - that's factually correct. But after the breach, 23andMe reset all passwords and required customers to use multi-factor authentication, which was only optional before the breach. Optional? Again, do your users a favour and help them protect themselves! If you don't, it may come back to haunt you.

Parting thoughts…

So, what's the 'theoretical' risk of an organisation exposing your confidential data? Victorina Police made that risk real this quarter by linking "over 11,000 cybercrime incidents" to the Medibank breach.

Finally, we often use the "NIST" framework for maturity reviews and roadmaps. A new "Version 2.0" was released and includes a new 'function' called "Govern" which stresses that leaders should consider cyber as a major enterprise-wide risk; placing it on the same level as legal, financial, and other forms of enterprise risk. Version 2.0 also places a greater emphasis on cyber supply chain risk management. Just let us know (here) if you want to discuss the implications for your organisation?

Thank you for investing the time to catch up with us this quarter! If you're not already, please 'follow us' on LinkedIn and/or Twitter (X), 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