It was a tumultuous quarter in politics... again! In July, we were thrilled to participate in a noteworthy event that brought together some of Australia's most influential business leaders with the (then) Prime Minister. The goal was explained well by Tobias Feakin, because the idea was borne out of response to "*what will help advance and grow the nature of the discussion on cyber security within Australia*?" His reply was "*it requires a prime minister who will be prepared to champion this issue and spend some time talking about it with those that can make a difference.*"

Indeed, this was an exceptional suggestion and inspirational to see it come to fruition. We think the success of Australia's future rides not only on its ability to innovate and embrace the digital era, but do so without naively exposing our intellectual property or private and confidential data to those seeking to exploit it.

In addition, Jennifer Westacott (CEO of the Business Council of Australia) who chaired the meeting explained "*because we all share the consequences of cyber crime, working together is critical... Australia is well placed to succeed with an agile and transformative strategy and now is absolutely the right time to act on this. If we take action we can ensure that we are not only open for business but one of the most trusted business environments in the world.*"

Well, we now find ourselves at the end of the quarter, and we have (another) new Prime Minister and Cabinet. The cyber threats we face haven't missed a beat and continue to accelerate. Politics aside, we're cautiously optimistic that the 'baby isn't thrown out with the bath water' and the new Leadership will embrace, if not accelerate, the positive steps take thus far.

Number nirvana...

This month we were shown an interesting new website from Lloyds that calculates overall risk in terms of the potential impact on economic output (thanks Andreas!). 301 cities facing risk from 18 manmade and natural threats.

There's a wealth of data, but overall if we see the 'glass half full' merely 1.2% of Australasia's GDP is associated with cyber risk – pretty small in percentage. Alternatively, if we see the 'glass half empty', Sydney and Melbourne are in the Top 20 global cities (12th and 15th respectively), for cyber attacks. In aggregate, $19.5 Billion of Australia's GDP is at risk from cyber attacks (that's a big number!).

While those numbers provoke interesting macro-economic discussion, a practical perspective was found in an insightful (albeit contrarian) article this quarter that "*There is no one-size-fits-all answer. Every business should resolve the issue based on an assessment of its own unique circumstances and risk...*" Drop us a note if you'd like to explore what that might mean for your unique circumstance.

'Voluntary' breach notification breaches your fiduciary duty?

If a Board, without legal obligation, chose to make a public announcement that caused customers to leave, or that hurt the financial results / viability of the company, would they have breached their fiduciary duty? Might it also open themselves to a shareowner lawsuit?

Numerous surveys say customers will leave a company if that company lost their personal or sensitive data. So therefore, if Australia has 'voluntary' data breach notification, what Board (in their right mind) would voluntarily notify customers of a data breach? Traditional product liability might imply some obligation, but 'information,' is not tangible and is often a secondary by-product...

That issue, in addition to the related challenges is the key topic of an industry panel discussion hosted by the American Chamber of Commerce. Trusted Impact's CEO join's three very impressive industry experts to explore this further on Wednesday 28 October – we'd be delighted if you were able to join the conversation!

What really happened in 2013

Brian Krebs, a top security reporter, and source of great security insight, published some very damning information this quarter about the 2013 Target Breach, which further highlights a reoccurring theme we find all of the time.

In particular, "*while Target has a password policy, the Verizon security consultants discovered that it was not being followed. The Verizon consultants discovered a file containing valid network credentials being stored on several servers. The Verizon consultants also discovered systems and services utilizing either weak or default passwords. Utilizing these weak passwords the consultants were able to instantly gain access to the affected systems.*" If you think this is unique, we have the factual statistics to demonstrate that it isn't. And it's likely that your organisation faces the same thing... a short, diagnostic effort can provide you with the facts you need to solve this. Call us.

In addition, it showed that although there was a *"...comprehensive vulnerability scanning program in place... remediation procedures did not address findings... in a timely fashion, if at all*". Getting insight into vulnerabilities is great, but only useful when resolved. Unfortunately this too is not unique. Don't be the next 'Target'.

If you're going to the cloud, a good analogy you can use

We got great feedback from one of our "LinkedIn" posts this quarter on going to the cloud, so we thought it might be useful to repeat it. We post other insights on a more frequently there. We'd be thrilled if you 'followed us'.

Putting your data into "the cloud" is a lot like staying in a hotel. Good facilities (pool, etc), your room's kept tidy, and you can upgrade if you need more space. But also, the 'staff' have a master key to your room, a party can ruin your stay, and you can land in a shabby hostel in the bad part of town.

Choose a cloud the same way. If your data's valuable, put it in the safe. If there isn't one, don't stay there. Make sure there isn't a party above you, and don't just assume all clouds have 'doors' or even sprinklers in case of a fire... it's all about the data... "There is no cloud, it's just someone else's computer."

Analogies are a good aid to understand 'the cloud' and how it might introduce risk to your organisation. Another powerful way is to analyse the public cloud services your staff are **actually** using (versus what you **think** they're using). Conducting a 'cloud discovery' exercise is a simple and inexpensive, yet highly effective, fact-based analysis to better understand your organisation's **real** cloud risk profile. The results always reveal big surprises, and debunk general myths held across the organisation. Send us a note if you'd like to understand more.

Just the facts...

We've always promised to only send this quarterly, and never more than 1 double-sided page... so not much room left this quarter. The two most impressive stats we saw this quarter are:

- 93% of UK consumers support mandatory breach notification laws
- Cybercrime will cost businesses over $2 TRILLION by 2019

Thank you for investing the time to read this quarter's newsletter. Please feel free to forward to colleagues.

TrustedImpact
PROTECTING DIGITAL

we're **independent** consultants – it's about **your** business and **your** success
with a **singular focus** – information security is all we think about
leveraging **experienced** professionals – credentials, not checklists