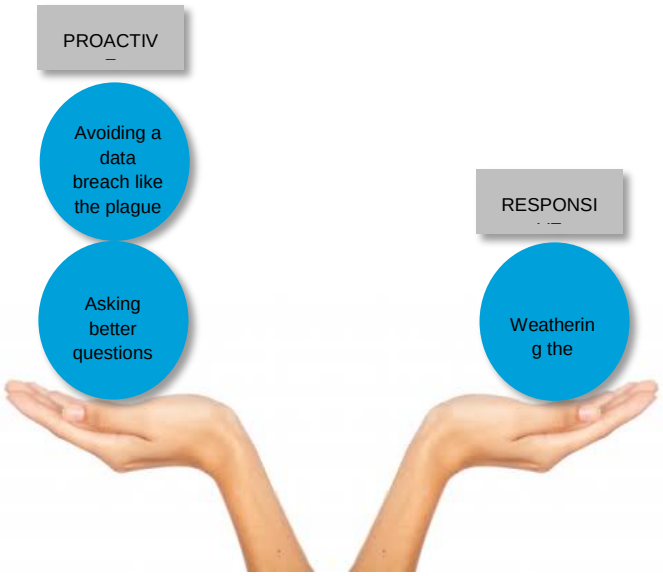
Cyber Security

NOT JUST ABOUT HACKERS ANYMORE!

Cyber Security: not just about hackers anymore.

We are living in a volatile age. Revelations and hacks are now daily fodder in the media and business community. So what's this got to do with your business? Cyber security is the next wave of risk and too many businesses are in the dark about the data they hold. And cyber security isn't just about data hacks anymore; it's not just about having a shield (a guard, as a firewall). Now, it's about having a sword (being armed, at the ready). Assurance, tax and advisory firms are publishing on the topic. They're not only highlighting threats to critical data by sector, but illuminating potential 'crown jewels' of an organisations' data bank, and surveying their clients' pain points around this.[1] The information is out there, and so are some compelling statistics around companies' levels of preparedness for the surge of data related issues – or lack thereof. But how does this fit with new Australian Privacy Laws as of February 2018 and your business's overall outlook on risk? What crisis management and what communication strategies are in place so that you can 1) avoid a data breach like the plague, and/or 2) weather the storm? We share some Proactive questions that you could be asking to get on the front foot with the new laws.



First, what do Olympic Gold and Fitbits have in common?

Here are some thought starters for contextualising data within your world and business.

- Take Shaun White. 2018 American Winter Olympics gold medallist. Yes, he can lock down a men's halfpipe in Pyeongchang, but what about the lock down on his text messages? The glory of his Olympic win had a shadow: the allegations of sexual harassment, including leaked text messages of an explicit and pornographic nature. So, we learn that performance can be tainted by data.
- Wearable technologies (eg Fitbits) are everywhere; most people have endorsed them. Smart phones are even more common place. The data these devices store and capture is extremely helpful! We've moved from a mobile phone that holds a contact list of your nearest and dearest, to a machine that acts as camera, personal credit card, knows your preference in entertainment and food, and has geotags for your location at any point in time. The fire power in your smart phone is largely dependent on the Apps you have. There are Apps that track your sleeping, your mental health and your finances. How would you feel if this data were to be 'lost' in cyber space?
- Now put this altogether into a business setting: think about which organisations have your personal details, including address, bank details, your child's details etc. Consider your private information leaking into the public domain: or into the hands of those who you never authorised to have your information. *This* is what's at stake.

[1] See Grant Thornton's published 2017 Report 'Locking down the value of data'.

It seems a kind of "data negligence" is the next frontier. After all, **negligence** = duty of care + breach + causation + damage. The new privacy laws are certainly saddling businesses with new duties, and penalties for breaches. But what exactly are the New Laws and businesses' new obligations around data and cyber security?

New Privacy Laws 101

The new Privacy Laws hinge on 1) access, 2) disclosure and 3) loss.

As an extremely simple example, Australia is now legislating on the situation where you leave your work laptop in a cab, and then reporting that incident for risk of exposing personal details, as held by your organisation. In essence, the new legislation is catalysing businesses to enact policies to protect their data storage and data flow. So, it begs the question of how your organisation interacts with its data. If "a business today is only as good as its data",[2] here are some worthy considerations for a quick pulse check within your company:

- What data are we creating and gathering?
- How much data is there in our company?
- What does our data 'do'?
- How secure is our business' Cloud storage, or similar?
- What harm could our data cause if our data is compromised?

On this question of harm, loss and disruption may loom large. Loss of monies. Loss of trust. Disruption of business operations. The impact on reputation and IT will almost be inevitable. Clearly people will be left exposed, and external stakeholders will have 'questions' (to put it politely!). Business' sites may also become jeopardised. The processes your organisation deploys in these instance are vital: as is the thinking and planning in advance.

Home soil snapshot

In February 2018 the new Privacy Laws came into place in Australia. The new laws introduce mandatory notification system for breaches of data, with noncompliance carrying significant fines.

DATA BREACH =	$$$ PENALTIES
• Unauthorised access or disclosure, or loss, of personal information held by an entity. • An entity has **30 days** to investigate whether a suspected data breach has in fact occurred • Once an entity is aware of a qualifying data breach, they must notify the Office of the Australian Information Commissioner **as soon as practicable.**	• Up to $1.7 million for breaches by corporations • Up to $300, 000 for breaches by company directors

Foreign soil snapshot

In May 2018 the European Union is introducing General Data Protection Regulation. In many circumstances this new EU data privacy law will put Australian businesses at risk of significant fines for noncompliance.

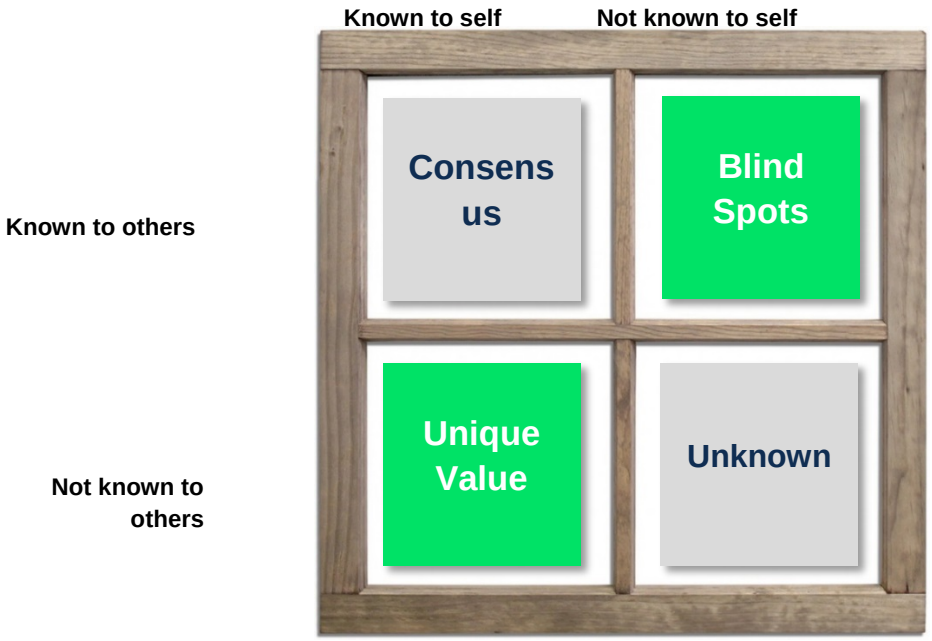
EXAMPLE	$$$ PENALTIES
• Australian business with an establishment in EU • Goods and services offered to EU customers	• Up to €20 million • Up to 4% of annual global turnover

[2] Grant Thornton, 2017

A Window into Cyber

While human behaviour does not have an algorithm, or code, it does have 4 core interlocking perspectives. The quintessential Window[3] model, borrowed from psychology, can help us ask 4 corresponding questions to frame the window for understanding human behaviour. And in an age obsessed with answers, sometimes it's about asking the better questions.

- What do I know that others also know? We call this **Consensus.**
- What do I know that others do not know? We call this **Unique Value.**
- What don't I know that others do know? We call these **Blind Spots.**
- What don't I know that others also don't know? We call this the **Unknown.**



Applying this thinking to cyber security and data:

CONSENSUS	The new privacy laws set new parameters for everyone, and it's time for your business to upskill.
UNIQUE VALUE	What unique value sits in your business' data, which is protected, private and confidential? Or is it?
BLIND SPOTS	What might be your blind spots regarding the new laws and cyber security/data management generally? When did you last actively turn around and check beyond the rear view and side mirrors?
UNKNOWN	This is where it's important to draw an informed line between what your business knows, and what it doesn't: ie, being crystal clear on knowing what you don't know.

[3] The Johari Window, Luft and Ingham (1955)

The really interesting impacts in a business setting are those which have uneven knowledge (green squares): ie either you or the other party is at an advantage or disadvantage. Asking these questions is an early step towards gauging strategies you may need to consider for future-proofing your organisation in regards to cyber security.

Whether you consider proactivity or responsiveness (ie reactivity) to be a more relevant consideration for your business, the fact of the matter is that the rules of data and cyber security have changed. For more information about reducing your risk margin, or to have a conversation about what the new laws mean for your business contact Gavin or Craig at the Business Olympian Group:

gavin@businessolympian.com.au

craig@businessolympian.com.au

Written by Emily Knowles, Specialist Consultant, Business Olympian Group.

Attributions, in order of appearance:

http://auminabox.com/the-big-mac-economy-how-the-hamburglar-stole-the-gdp/ citing Hamburglar art credit: Rog Hernandez, http://roghernandez.blogspot.com

https://www.espressoenglish.net/18-idiomatic-expressions-with-hand/

Grant Thornton (2017). Locking down the value of data.

KPMG (2017). Privacy Change is Coming.

Craig Goldberg – 0419220707 – craig@businessolympian.com.au
Gavin Freeman – 0413043417 – gavin@businessolympian.com.au

ABN: 25 659 508 957

PO Box 628
Bentleigh East, VIC, 3165

www.businessolympian.com.au