tate PARTNERS
ACCOUNTING & ADVISORY

Beyond Numbers

February 2019

What would happen if….

Life does not always go to plan. While we logically know that, most of us don't plan for the worst - it's all a bit morbid and time consuming.

The downside of not planning is the potential for hard earned assets to be squandered, family fall-outs, and money handed to the Government that could have been distributed in accord with your wishes. If you are a business owner, then the stakes are even higher.

As a population, planning is more important than ever because:

The ageing demographic – 1 in 7 of us are now aged 65 and over (3.8 million)
The baby boomer generation represent only 25% of the population but hold 55% of the wealth
We are entering a period of intergenerational wealth transfer from the baby boomer generation
Over the last 25 years there has been an explosion of wealth in Australia

Estate planning is simply identifying your assets and liabilities and what you want to happen to those assets if something happens to you. As part of that, you need to look at the issues that might arise and how best to manage them. All of this is then reviewed for tax outcomes and the legal requirements to provide the best care and protection for your beneficiaries.

If you are a business owner, there are also another set of issues to consider to ensure that the business can continue if you are not able to continue in your current role. Or, your beneficiaries can take their share of the value accumulated in the business. This planning will protect your beneficiaries, the business, and your business partners.

Estate planning does not have to be hard work, but it does have to be planned.

It's also important to understand that actual wealth or the size of your estate is not the sole reason for estate planning. Estate planning is important for:

- The care and maintenance of minor children.
- Managing the respective rights and expectations of beneficiaries, particularly with blended families.
- Avoiding disputes between family members.
- Relationships outside of the immediate family.
- Managing liabilities of the estate.
- Assets which may not be capable of immediate realisation or where value will be diluted by realisation.
- The transfer of assets through generations.

Estate planning seeks to not only distribute the assets of your estate but do so in a way that protects the estate, addresses issues within the estate, and fulfils your wishes.

What the stats say

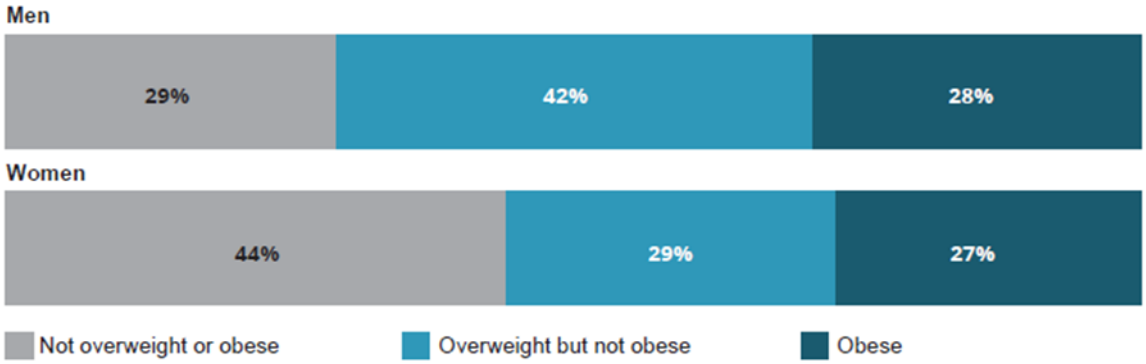
While 4 in 5 of us rate our health as 'very good', 50% of Australians have a chronic condition that is likely to cause their death, 63% of adults are overweight or obese, and around 45% of us will experience a mental illness in our lifetime.

Leading causes of death differ by age:

- 1–44 years: suicide, land transport accidents
- 45–74 years: coronary heart disease, lung cancer
- 75 years and over: coronary heart disease, dementia and Alzheimer disease

It's estimated that 138,300 people were diagnosed with cancer and 48,600 died from it in 2018.

Proportion of adults who are overweight or obese:



Australia enjoys one of the highest life expectancies of any country in the world at 82.5 years (in 2015) and is ranked fifth among 35 OECD countries. Japan has the highest life expectancy at 83.9 years.

Men aged 65 in 2014–2016 could expect to live another 19.6 years (an expected age at death of 84.6 years) and the life expectancy of women aged 65 in 2014–2016 was 22.3 years (an expected age at death of 87.3 years).

We're also working longer – 13% of Australians aged 65 and over participate in the workforce (17% for men and 10 for women). This is compared to 2006 when the workforce participation rate was 8%.

Tax warning on overseas income

Do you earn income overseas? A recent case highlights why you might pay more tax than you thought on foreign income.

If you are an Australian resident and earn income from overseas, such as income from investments, sale of assets such as property, distributions from foreign trusts, etc., you will generally need to declare that income in your Australian tax return. If you have paid tax in a foreign country on that income, you might be able to claim a foreign tax offset to reduce your Australian tax liability.

Sounds simple enough but a recent case highlights where problems can occur and you might end up paying a lot more tax than you thought.

The taxpayer in this case was a resident of Australia but was taxed in the US on gains they made on interests in US real estate. Most of the gains they made were taxed at a concessional rate of 15% (rather than the normal rate of 35%) because the interests had been held for more than one year. Some of the gains were ultimately taxed at 35% in the US.

The capital gains were also taxed in Australia and qualified for the general CGT discount of 50%.
As the taxpayer was a resident of Australia and had paid tax on the US gains, the taxpayer claimed a foreign income tax offset for all of the US tax they paid. However, the ATO amended the tax assessment and only allowed a tax offset for slightly less than 50% of the tax they paid in the US.

The problem for the taxpayer was that while the US and Australia both have tax concessions for longer term capital gains, they operate quite differently. The US applies a lower rate to the whole gain while Australia applies a normal tax rate to half of the gain. Unfortunately for the taxpayer, the Federal Court held that the Commissioner's approach was correct. If foreign tax has been paid on an amount that is not included in your assessable income then you cannot claim a foreign tax offset on it. In this case, the portion of the capital gain that was exempt from Australian tax because of the CGT discount, was not included in assessable income.

It is not uncommon for people who have made capital gains on foreign assets to assume that they get all of the tax back that they paid overseas. Unfortunately, that's not necessarily the case and often only a partial credit is available, if at all.

What changed on 1 Jan 2019

- Tampon tax (GST on sanitary products) scrapped
- Voluntary crackdown begins on credit card providers to protect consumers who cannot pay-off their credit card debt or who cannot afford an increased limit
- Higher Education Loan Program:

⇒ New lifetime caps prevent students repeating courses or continually enrolling in new courses.

⇒ New loan limits: Increase in fee assistance for students studying medicine, dentistry and veterinary science courses with increases in their loan limit from an estimated $130,552 in 2019 to a new limit of $150,000. $104,440 for all other students.

You've been scammed, hacked or breached!

Another year, another scam. While data driven crime is more sophisticated and difficult to address than ever, human error and judgement remains one of the major problems.

The latest data breach report from the Office of the Australian Information Commissioner (OAIC) is surprising for the simplicity of the problems - 37% of data beaches resulted from human error not malicious attack. In over 20% of reported cases, personal information was simply sent to the wrong recipient. Another 6% of complaints were attributed to system faults.

Since 22 February 2018, businesses covered by the *Privacy Act* need to report unauthorised access to or disclosure of personal information or loss of personal information that your business holds under the Data Breach Scheme. The rules impact organisations with an annual turnover of $3 million or more, businesses 'related to' another business covered by the *Privacy Act*, or if your business, regardless of size, deals with health records (including gyms, child care centres, natural health providers, etc.,), is a credit provider, or holds Tax File Number information.

Organisations are required to take all reasonable steps to prevent a breach occurring, put in place the systems and procedures to identify and assess a breach, and issue a notification if a breach is likely to cause 'serious harm'.

What the statistics from the OAIC demonstrate is that procedural integrity in your business is paramount – train your team to not only be wary of scams but ingrain best practice for the day to day management of personal data. Privacy protection is not just an 'IT' issue.

While not the only factor, protecting your systems remains a priority as Marriot Hotels discovered when the Starwood guest reservation database was breached. According to the latest announcement, up to 383 million records were potentially impacted. Of those, there were approximately 5.25 million unique unencrypted passport numbers. On 30 November 2018, the company announced that unauthorised access to the database may have been occurring since 2014.

Similarly, Cathay Pacific released a statement notifying that up to 9.4 million members of their Marco Polo Club, Asia Miles or a Registered Account holder have potentially had their data breached including passenger name; nationality; date of birth; phone number; email; address; passport number; identity card number; frequent flyer programme membership number; customer service remarks and historical travel information.

Remember, hackers can gain access to your business's data simply by a staff member clicking on a link.

While not impacting personal data, according to the ScamWatch, a common scam is where hackers gain access to a business' email accounts, or 'spoof' a business' email so their emails appear to come from the company. The hacker then sends emails to customers claiming that the business's banking details have changed and that future invoices should be paid to a

Australian Government
Australian Taxation Office

new account. These emails look legitimate as they come from one of the business's official email accounts. Payments then start to flow into the hacker's account. The average loss from these scams is around $30,000.

A variation is where the hacker sends an email internally to a business' accounts team, pretending to be the CEO, asking for funds to be urgently transferred to an off-shore account. Hackers can also request salary or rental payments be directed to a new account.

In 2018, these scams cost Australian business $30 million in 2018.

Simple measures you can take:

- Have strong and enforced processes in place for the management of personal client information.
- Strong authorising procedures for payments – two-step authority.
- Change passwords often and use two-step authentication where available.
- If a client's bank details have changed, phone them and check the details.
- Train your team on cyber security:

⇒ Check requests for payments that arrive electronically from other team members and management.

⇒ Check email addresses are legitimate – look for slight variations.

⇒ Be suspicious of poorly written emails.

⇒ Don't click on links from email – always use your account with the supplier or Government department to check details.

- If contacted by the ATO, contact us to verify

Latest scams

ATO scams

The Australian Taxation Office (ATO) has warned about the emergence of a scam where "…scammers are using an ATO number to send fraudulent SMS messages to taxpayers asking them to click on a link and hand over their personal details in order to obtain a refund."

The refund scam follows a more sinister four phase scam stating there is a warrant out for your arrest for unpaid taxes in prior years. The scam starts with a text message purportedly from the Australian Federal Police (AFP). Within minutes, your mobile rings and the caller identifies themselves as being from the AFP and working with the ATO. They then ask for your accountant's details. You then receive a call purportedly from your 'accounting firm' asking you to verify the AFP/ATO claims. Finally, you are provided with a way, if you act quickly, to make the AFP go away by paying a fee before your 'imminent arrest'.

The ATO states that it will not:

- send you an email or SMS asking you to click on a link to provide login, personal or financial information, or to download a file or open an attachment;
- use aggressive or rude behaviour, or threaten you with arrest, jail or deportation;
- request payment of a debt via iTunes or Google Play cards, pre-paid Visa cards, cryptocurrency or direct credit to a personal bank account; or
- request a fee in order to release a refund owed to you.

Medicare Scam

A new phishing scam sent text messages purportedly from Medicare advising the recipient that they are owed a $200 rebate from Medicare. Once the person clicks on the reclaim link, they are asked to provide their personal details including bank account details for the 'rebate.'