Brokerwise™

YOUR INSURANCE BROKER

News about issues that affect your business

Issue Two. 2017

INSIDE THIS EDITION

End of Financial Year Checklist

It's that time of year again and the End of Financial Year is upon us. Before 30 June take a moment to review your business so you can start the new financial year off on the right track.

1. Review your business story
How has your business changed in the past year? As your business evolves to cope with your clients ever increasing expectations and technology advancements, consider any improvements you made and if this has now changed your goals.

Do a financial health check to consider your current cash flow, profitability and return on investment. If possible see if there are bench-mark figures for your industry available and compare your business performance to these.

Often, businesses forget to look at their systems and processes. Whilst it can be a tedious task to review and implement a new way of doing things, the long-term benefits of implementing something that will save you time, is a business win.

The aim of this exercise is to identify any weak-nesses you find and to develop a plan to ad-dress them. You don't need to do all the work yourself either, get your staff to help out and come up with ways to improve the business.

Actions out of this process should be documented, assigned to an owner and have clear timeframes agreed for resolution.

2. Have a clear strategy - Look at where you want to be in the future
Have a clear understanding of:
• How you are unique.
• Understand your industry, its unique qualities and opportunities.
• Understand your customer, who you are going to serve and how you are going to do it. You can't be everything to everyone.

3. Prepare a budget
Ensure that you have, or have access to, sufficient resources to achieve your objectives. Regularly monitor your actual results and identify the reasons for variations.

4. Cash flow is still king
Many businesses discover that even though their business is profitable, cash flow problems can be its downfall by stopping expansion plans or not having money available at the right time to increase staff or product lines.
Ensure you understand any seasonal fluctuations in your business and also ensure you have a good invoicing system. Most accounting packages can send out automated reminders to customers who are slow to pay or perhaps it may be necessary to allocate a little more energy to chase up older debtors.

5. Review your marketing plan
Is it achieving your objectives? Measure the success of each campaign or activity to determine its effectiveness. Increase focus on products with a high margin and reward your employees for achieving targets in your preferred areas.
The reward must be easy to understand and easily measured, monitored and communicated during the financial year.

6. Review your risk management plan
Some key issues to address might be:
• Major damage at your own, a key supplier or key customers premises. This could have a disastrous effect on your business.
• Loss of a key supplier.
• Failure of a key customer.
• Loss or illness of key staff members.
• Damage to your reputation through a social media attack.
Take some time to think about your options, if any of these, or similar events occurred.

7. Don't be afraid to bring in the professionals
A lot of businesses make the mistake of not reaching out to the specialists when they need help. There are a wide range of specialists, from business coaches, accountants, marketers, investments advisors etc. out there ready to help you achieve your objectives and keep you on track.
Finally, although it may appear hard, it will put you in a good position to explore new opportunities, minimise risk, maximise profits and help you sleep better at night.

Brokerwise™

Mandatory data breach notification laws to come into force

Parliament has recently taken steps to address issues relating to cybercrimes by passing the *Privacy Amendment (Notifiable Data Breaches) Bill 2016* on 13 February, 2017. The legislation is due to commence within 12 months of Royal Assent, with no assent or fixed date as yet. However, once enacted the legislation will amend the *Privacy Act 1998* to require entities experiencing 'eligible' data breaches to notify affected and 'at risk' individuals and the Office of the Australian Information Commissioner (OAIC) of these breaches.

The new laws will apply to entities which carry on business in Australia or are subjected to the *Privacy Act 1998*, including businesses and not-for-profit organisations with an annual turnover of $3 million or more, credit providers, credit reporting bodies and entities that hold the tax file number information of one or more individuals.

An 'eligible' data breach is:

- Unauthorised access to, or unauthorised disclosure of, personal information held by an entity and a reasonable person would conclude that access or disclosure would be likely to result in serious harm to any of the individuals to whom that information relates; OR
- Information is lost in circumstances where:
    a. Unauthorised access to, or unauthorised disclosure, is likely to occur; and
    b. Assuming such access or disclosure were to occur, a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom that information relates.

Whether access or disclosure would likely result in serious harm depends on a number of factors, including the nature and sensitivity of the information, whether there were any security measures in place and the likelihood those measures could be overcome, the characteristics of the person obtaining the information and the nature of the harm suffered by the individual.

If an entity suspects that an 'eligible' data breach has occurred, the following steps should be taken:

1. Within 30 days of the suspicion arising, assess the relevant circumstances and whether it reasonably amounts to an 'eligible' data breach;

2. If there are reasonable grounds to believe an 'eligible' data breach has occurred then subject to a number of exceptions, an entity should prepare a statement setting out the contact details of the entity, a description of the breach, the kind of information concerned and the steps it recommends affected individuals take in response. A copy of this statement should be provided to the OAIC;

3. If practicable, take steps as are reasonable in the circumstances to notify affected and 'at risk' individuals of the contents of the statement. If direct notification is not practicable, the entity should publish the statement on its website and take reasonable steps to publicise the contents of the statement.

The OAIC may also give written notice to an entity directing it to prepare the statement if it is aware there are reasonable grounds to believe that there has been an 'eligible' data breach.

The failure to comply with the new laws will effectively be regarded as a breach of the *Privacy Act 1998* and can result in an entity being required to take remedial action, give enforceable undertakings and pay compensation and/or fines of up to $360,000.00 for individuals and $1.8 million for corporations.

Businesses should now review their internal processes, resources and systems to ensure they can adequately respond to any potential data breaches in future. As part of this review process, we suggest contacting your broker to ensure you have adequate insurances in place for any potential cyber and privacy breaches.

Protecting against cyber predators

On May 13, 2017 many internet users in the UK, Europe and Russia woke to a major Ransom Cyberattack. The USA was lucky, they were able to stem the outbreak, but the total number of people, companies and Government bodies effected may never be known.

Hackers don't care who it affects and we are all vulnerable and potential targets as the internet and email are two essential tools that are used to run and grow your business. Equally they can be one of the easiest paths to severely disrupt or ruin your business.

These international data crime gangs use sophisticated methods and systems such as malware, ransomware and data phishing, which are all aimed at infiltrating your systems and hijacking your data. With the plan to steal usernames, passwords, access your accounts and pins, make purchases, or simply sell information about you to other parties for use in illegal purposes. Their goal is money with no thought of their victim's ruined credit rating, lost money and ruined lives.

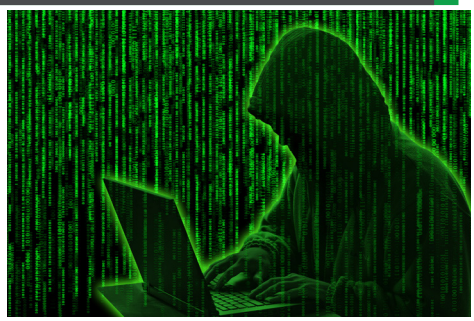
If your computer is successfully hacked and data locked up, the criminal's promise to return your data is usually subject to payment of a ransom demand, usually Bitcoins; and in some circumstance even if payment is made, your data may not be released.

Whilst Australian law enforcement authorities state that the smaller ransom demands are known by the criminals to be more successful, as those affected are prepared to quickly pay small amounts and not report the problem, demands in the thousands of dollars have been seen recently in Australia in the small business sector.

Microsoft had already issued patches but many users do not always immediately install updates or are still operating on old program versions for which no updates are available.

There are actions you can take to reduce your risk to these gangs, protect your systems and your business. Industry specialists recommend these actions to protect against cyber predators:

- Use a firewall.
- Update your system regularly.
- Use up-to-date program versions.
- Increase your browser security settings.
- Avoid questionable websites.
- Only download software from sites you trust.
- Use antivirus protection.
- Install antispyware protection.
- Use a pop-up blocker.



Most importantly, instigate a regular data back-up regimen with at least one copy off site. In addition, Cloud storage via Dropbox or similar services is a growing and reliable option.

When all else fails, further protection is available in the form of new and developing insurance products that can help you pick up the pieces following a cyber-attack event.

As software developers know, hackers develop viruses and intrusive encryption systems even before a new piece of software is released to the market. Do what you can to keep your commercial information safe and talk to us, your broker about what covers are available to stay one step ahead.

Cyclone Debbie - the good and the bad

As the state continues to recover from ex-Tropical Cyclone Debbie, the real cost of the cyclone quite possibly will never be known.

The cyclone, which crossed the coast on 28 March, 2017 as a category-four system and caused subsequent flooding in communities from the Whitsundays to New South Wales and then across to New Zealand. Over 72,000 Queenslanders requested assistance.

And while PERILS, the independent Zurich-based organisation providing industry-wide catastrophe insurance data disclosed its initial property market loss estimate for Debbie at $1.116 million, there are other losses that are just not counted.

Cyclone Debbie caused the closure of many schoools in Queensland for two days and many businesses also closed in the lead up. Once the Cyclone past, many of the affected areas had further closures as a result of public utilities.

Business owners wore the cost of the closures with these figures unlikely to be ever known.

While many analysts expected the cyclone to have minimal impact on broader economic growth, there was severe damage to sugar and fruit and vegetable crops causing shortages in supply.

A quarter of all sugar produced in Australia comes from the Mackay-Proserpine region, with the Bowen region also a key producer of fruits and vegetables including mangoes, tomatoes and capsicum.

But there are some postivies that have come from Debbie including the fact that emergency services including the SES and volunteers who did a marvellous job during the disaster.

More coverage

In comparison to Cyclone Yasi in 2011, Queenslanders now have wider insurance coverage options available.
It is important to have a broker assist and talk to you in handling the claims process.

With reports of policy holders being scammed by people, doorknocking at homes, claiming to be representing Insurers and demanding cash payments to clean up, inspections and repairs. No Insurer's representative would ever demand cash for such work.

These scams highlight the importance of having a broker who can assist with the claim process in what is a stressful situation.

Travel smart and travel safe

Passport – check. Clothes – check. Medications – check. Smartphone – check. You've got all of the above, but what about travel insurance?

Travelling overseas can be a fantastic adventure – but you shouldn't do it without first having a travel insurance policy in place.

Not all travel policies are the same with many policy limitations that sometimes aren't as obvious until it's too late. It's vitally important to ensure that you're purchasing a policy that is adequate for where you are going together with coverage for activities that will be undertaken.

Many activities are not included in the "standard" policies for example heli-skiing or caving or certain underwater activities may be excluded or have policy limitations imposed. Be careful to ensure that any activities you intend to undertake are covered prior to your departure.

Further, you should also make a point of looking up the Government's smart traveller website to check the "safety status" of the country you intend visiting. This official site classifies countries according to travel safety and, of course, in many parts of the world this is volatile and subject to constant change.

The highest warning the Government issues is its "Do Not Travel", which advises against travel to certain destinations. Some current "Do Not Travel" warnings include Syria, Afghanistan, Iraq, South Sudan and Yemen. Be aware that if you travel to countries against advice, your travel insurance will most likely be voided. A number of countries are on a "Reconsider your need to Travel" list.
While your travel insurance will usually provide coverage in this case violence, political unrest and terrorist activities can escalate quickly, and may force the Australian Government to upgrade its warning to "Do not Travel".

To ensure that you have the appropriate travel insurance its prudent to discuss your requirements with us, so we can tailor a policy accordingly and arrange well prior to your departure date.

Creepy crawly spider facts

DID YOU KNOW?

- You are rarely more than a few metres from a spider. And that one acre of ground is home to about a million spiders!
- Around most homes you will find about 20-50 different species of spider. But in any bushland area, there is usually around 100-120 species!
- There are around 10,000 different species of spiders in Australia, but only around 3,500 have names - but don't be alarmed, most are too small to bite.
- And it is the unexpected direction that spiders move in that generates the fear response in humans.
- The majority of spiders will run away from wind/blowing.
- If you have a 4WD watch out - spiders (as well as scorpions, cockroaches, lizards and snakes) are attracted to an idling 4WD diesel.
- Speaking of cars...although huntsmen spiders have a weak venom, they are responsible for the most human deaths through car crashes (as they scramble across the windscreen).
- Spider silk is easily dissolved with household bleach
- Despite popular belief, daddy long legs spiders are harmless..
- Male spiders look and behave like females until they are adult.
- No Australian spider (including the white tail spider) has caused flesh-rotting.
- An Australian jumping spider, Portia, has telephoto vision second only to the eagles.
- Most spiders have eight eyes but are basically blind.
- Spiders often consume their webs at nights end and then recycle the silk, through their gut, in about 20 minutes.
- Most of the white on a spider is formed by the white guanine in the folds of the gut
- Spider silk is highly elastic so when it reaches its most stretched point in the Spiderman movies, it should pull him straight back to base, not act like a rope.

Wisewords

"Don't be afraid to give up the good to go for the great."
— John D. Rockefeller

"In order to be irreplaceable, one must always be different."
- Coco Chanel

"In the middle of every difficulty lies opportunity."
- Albert Einstein

Your Insurance Broker

ABN 90 825 731 321 AFSL No. 244335

12 Baldwin Street
(PO Box 1444)
Caloundra QLD 4551

Phone: 07 5491 9000
Fax: 07 5491 9299
Email: manager@yib.com.au
Web: www.yib.com.au