AIS Liaison
The AIS Insurance Brokers Newsletter
WINTER 2019

Understanding the building crisis

You know things have reached a critical point when governments don't just start talking about an issue – they immediately act on it.

The issue of the moment that has forced governments to act is the crisis of confidence in the building industry's construction standards. We are all familiar with the fears surrounding apartment and commercial buildings clad in flammable panels, but the problem doesn't stop there. The evacuation of several apartment buildings in Sydney after cracks appeared in their structures is an indication of just how deep the problem is.

The New South Wales Government has started a parliamentary inquiry into the troubled sector, while in Victoria a $600 million rectification plan for private high-rise towers that carry flammable cladding is about to begin.

Inevitably insurance has been caught up in the mayhem. As News Limited business commentator Alan Kohler put it recently, insurance is "the canary in the coalmine".

Politicians had taken nearly a year to seriously discuss the Shergold Weir report on improving compliance and enforcement of building codes. But when insurers began to impose tough restrictions on building surveyors' professional indemnity (PI) insurance, governments were forced to respond immediately.

At the Building Ministers' Forum in July, the federal and state governments finally committed to all 24 suggestions in the Shergold Weir report.

Cladding alert: fire raced up Melbourne's Lacrosse building in 2014

However, the insurance industry is maintaining its tough stance, waiting for action to follow the ministers' pledges about lifting building standards and regulatory oversight. In the meantime, getting suitable PI cover or renewing an existing contract is becoming increasingly tough for building professionals.

Not only have premiums risen alarmingly quickly – in some cases more than doubling – underwriters are imposing tougher conditions and in many cases demanding a comprehensive risk management program.

Certifiers and surveyors can no longer get exclusion-free PI covers. In those states where full cover has been a requirement for surveyors and certifiers, licensing conditions have had to be temporarily relaxed to allow PI policies with exemptions.

This means that affected building professionals are now exposed to massive liabilities if anything they certify or approve is later found to be non-compliant with the standards.

The risks from non-compliant aluminium panels and flawed documentation extend into other forms of insurance as well.

"The presence of combustible cladding is likely to increase the amount of first-party property loss and third-party damage or injury in the event of a fire, a PwC report prepared for the Queensland Government says. "Public liability insurers are concerned about the risks posed to occupants and their property in the event of a fire involving non-compliant cladding, particularly where the building owners may be aware of the non-compliance."

There, in a nutshell, is how the building crisis is affecting insurance and everyone working in the construction industry. The danger is that without insurance, nothing can happen.

Making sure you have your liability bases covered – no matter what industry you work in – is especially crucial in these difficult times. Give us a call and we will help you sort your way through the issues.

How commissions work for you

The payment of commissions for financial services has received plenty of attention recently, with intermediaries in other parts of financial services coming under pressure after the Hayne royal commission.

The whole issue of commissions is now being examined by the regulator over the next couple of years, and we are confident that commissions paid by insurers to general insurance brokers do positively impact on the service we provide our clients.

Importantly, the role of insurance brokers is to always act in the best interests of their clients as they work to assess the suitability of various products in the market. Commissions received from insurers are typically paid on a similar basis no matter where cover is placed, taking the cost burden off clients without interfering with the "best-interests" duty.

The National Insurance Brokers Association has noted that alternative fee-for-service arrangements, such as expensive hourly rates in some professional areas, risk deterring people from seeking advice on the best ways to deal with risks and may have unintended consequences.

Brokers currently are able to take as much time as necessary to consider the client's ongoing circumstances, weigh up all risk transfer options and just as importantly assist at the time a claim is made – all without additional charge.

The claims side is often the forgotten part of the equation, but it's a key difference when it comes to general insurance and other financial products. Alleviating worries after a catastrophe hits your business is vital.

Vero's SME Insurance Index 2019, which surveys business owners, found 36% of small businesses use a broker to source their insurance, but even with the benefit of commissions some owners baulk at taking advantage of the advice available.

Those choosing seemingly quick and easy online options often find they are a false saving compared with using the expertise of brokers as trusted advisers.

It can be difficult to assess whether specific risks are covered by so-called direct policies, which are generic in nature. Any shortcomings are often not discovered until a claim occurs, which can mean taking a financial hit.

By comparison, we brokers are able to obtain a number of quotes from insurers in a fraction of the time it would take you, we can leverage our networks to negotiate a better price and we know how to assess and identify the specific risks of individual businesses and the sectors in which they operate.

Some risks can't be completely eliminated, but we can advise on the best options to minimise risks.

In the event you do have to make a claim, you're going to be very happy you've got a broker working for you. We represent you and only you, and we're there to ensure you get the best possible settlement, saving you the costly, time-consuming and often frustrating process of directly negotiating with insurers.

The debate over commissions in financial services will likely continue, but in general insurance at least you can be assured that commissions don't interfere with the fact that our sole focus is on our client. It's a way of making sure that small and medium-sized businesses are able to access affordable expertise.

Of course, you'll only get the benefits if you arm us with timely information. If you've made any changes to your business – bought new equipment or expanded into new areas for example – keep in touch with us to make sure we have all the information we need to protect your business in the best possible way.

Pay or don't pay? How to respond to ransomware

As the number of hacks and cyber attacks continues to rise, protecting the systems and data your business relies on is more important than ever. An increasingly common type of cyber attack is ransomware, which can have an instant financial impact as well as long-term consequences for the infected business.

The concept behind ransomware is simple. Hackers encrypt all the files, folders and drives on a device and then demand a ransom to be paid before they reinstate them.

Ransomware is cheap to deploy and widespread, so even if only a few victims pay, attackers will likely make a handsome profit. As such, cyber criminals attacking in this way will typically take a "scattergun" approach in targeting their victims.

Being attacked by a ransomware hacker is financially damaging for a business, and if it's handled badly, the damage to your company's reputation can be irreparable.

Here's what to do if your business is attacked:

Identify the weakness: Ransomware most often gets into a system through a malicious link or email attachment. In most cases it will only affect the device it was opened on. However, in some cases the entire system can end up infected.

The first step after an attack is to find the device that was infected first and work out if other suspicious emails have been opened on other devices. The sooner you find the source, the quicker you can act.

Disconnect your device: After infiltrating one device, ransomware can spread quickly through the network. So it's important to remove the infected machine from the office network.

Notify the authorities: It's important to notify the relevant authorities of a breach as soon as possible. But be aware that Australian laws are ineffective in the case of the perpetrator residing in another country. Checking the Australian Police website, www.afp.gov.au/cybercrime, will tell you that unless your attacker is operating from within the country, the police can't really help you. And if you have business contacts of any kind in the European Union, you must inform the EU Information Commissioner's Office within 72 hours, or face a significant fine.

Inform employees and customers: It's important to be transparent in the event of a breach. Employees should be made aware of it immediately and the actions that you are taking to resolve it. You should also let your customers know that their data may have been compromised in a ransomware attack. Customers will respond better to your business if they hear this news from you, rather than from the media.

Update your security: Once the incident has been resolved, it's important to audit and update your IT systems. This can be a bit of a financial investment, but it's important to ensure your data and company reputation stays intact.

Don't pay the ransom: A few years ago the number of ransomware attacks increased as cyber criminals realised a lot of people were paying up, and that they could make a significant amount of money for little effort. Worryingly, research found that one-third of companies believed it's more cost-effective to pay the ransom than to invest in a security system!

Be prepared: Before it happens to you, set up systems to repel online intruders and safeguard your IT security. Have a plan in place detailing the procedures you will take in the event that your business is attacked by hackers.

We're no strangers to the subject of cybercrime, and we will always be happy to share our knowledge with you. Talk to us about your cyber weak spots and ways we can help you protect your business and – if the worst happens – how we can help you with one of the growing number of cyber insurance policies that are available now in the market.

Cyber insurance can cover ransomware as well as many other potential attacks on your business IT and systems. Better an ounce of prevention than a world of pain.

Under attack: following best-practice advice is crucial in responding to ransomware

Taking control in the age of autonomous vehicles

Strap yourself in: driverless vehicles are just around the corner

In February this year the first open-traffic driverless vehicle trial in Australia was launched at the University of New England campus in Armidale, NSW.

The project is just one of many developments currently underway to revolutionise land transport as we know it. Road trials of self-driving cars have been going on in a number of US cities in the past few years, with Google, Apple and other technology giants at the forefront of the effort.

Nobody quite knows when autonomous vehicles will become mainstream. But there is consensus on one thing: they will eventually outnumber humans behind the wheel.

And nowhere is the driverless trend more apparent than at airports. The past few years have seen cities around the world deploying pilotless shuttle trains.

With the billions of dollars invested, driverless technology is advancing at a rapid rate, and it's only a matter of time before autonomous vehicles take over the roads. A Finity Consulting report published by the NSW State Insurance Regulatory Authority (SIRA) estimates annual sales of automated vehicles will account for 75% of all light-duty vehicles by 2035.

Now, 2035 may seem like a long time away, but 16 years isn't a long period of time at all. Not when there is a relentless race among tech giants and car manufacturers jostling to secure their placing in a market that is predicted to be worth as much as $US7 trillion by 2050.

There are many arguments in favour of autonomous vehicles. Not only will they be carbon emissions-free, machine-controlled vehicles will reduce the number of road accidents.

Put simply, robot drivers will be more skilled and more careful than human drivers.

About 90% of road accidents are caused by human error. SIRA estimates that fully automated vehicles will reduce vehicle driver and passenger injuries by 80%, cyclists by 70%, motorcyclists by 40% and pedestrians by 45%.

So as the age of autonomous vehicles edges ever closer, businesses big and small will have to adapt. And that is because a slew of legislative changes will have to accompany the introduction of vehicles that will do the driving for you.

Depending on how legislative changes and road tests progress, autonomous vehicles could happen faster than you think. How will that impact on your business? And on your everyday life? Probably quite a lot. It's just the same with insurance. As risk factors fall, so will premiums, which is good for everyone.

One thing that won't change is our ability to keep abreast of the very many ways the technological wave is going to change our lives and our businesses. With overwhelming change come new types of risk, and we'll always be here to help advise and help keep your business safe and secure. That's something that certainly won't change.

AIS

A.I.S. Insurance Brokers Pty Ltd

137 Moray Street
South Melbourne 3205
PO Box 7760
Melbourne Victoria 3004

Telephone: 03 8699 8888
Facsimile: 03 8699 8899
insure@aisinsurance.com.au
www.aisinsurance.com.au