

Dear valued client

This is a very worrying time for all of us with both our health and financial security at risk.

We acknowledge that all customers are facing a period of change and uncertainty so in conjunction with the insurance industry we are working on a range of initiatives and solutions to suit the specific requirements of each of our clients.

Should you find yourself facing financial hardship, we urge you to contact us as we can talk you through a range of measures to ensure your cover best meets your current needs.

We all need to act prudently, therefore sound insurance protection remains critical to all businesses, organisations and individuals.

A number of business owners are querying if they should cancel their insurance or are considering cancelling covers such as business interruption which they do not consider necessary, particularly when they have been told they have no cover as a result of the closures caused by COVID-19.

### What advice can I obtain from my Insurance Broker?

#### BUILDINGS, CONTENTS, PLANT & STOCK (MATERIAL DAMAGE)

This is a serious issue for individual businesses should they be hit by an insurable event and for the economy. Remember that Material Damage insurance responds to many other perils the business is still exposed to, such as fire, burglary/theft, glass breakage, malicious damage, storm damage, impact, earthquakes and other natural disasters including flood where insured.

Remember, just because your business is closed does not mean that fires, burst pipes, storms, burglaries or, if things get out of hand, civil unrest stop. If your business is in financial stress you may not be able to reinstate your assets and survive this crisis without the benefit of a Material Damage policy.

In addition, your business may have a finance agreement with your bank or another financial institution which contain covenants requiring the property used to secure lending facilities, remain adequately insured at all times.

Policy premiums can be reduced by volunteering an increased excess, but keep in mind this is most effective with significant property insurance portfolios where you can afford the additional exposure of having to pay for damage under the voluntary excess, and the insurer offers a meaningful reduction in premium costs.

## BUSINESS INTERRUPTION

Business Interruption policies respond to cover the financial consequences (reduction in profit or increased costs) following a claim for which cover is provided by the Material Damage policy. The potential for a loss to occur that not only causes physical damage to property but results in a long term (sometimes months or even years) financial loss remains.

Our strong advice is to retain business interruption coverage. We do not know how long the closures will remain in force. The way a business interruption policy works is that a loss would be paid based on the standard turnover which is typically defined as “The Turnover during that period in the 12 months immediately before the date of the Damage which corresponds with the Indemnity Period” of the business with adjustments for the trend and special circumstances that effects the business but for the loss.

The best strategy in respect of business interruption is to use the premium adjustment clause and at renewal provide a declaration of the actual gross profit of the business and seek a return of premium if warranted. Most policies provide up to a 50% adjustment. In addition, many insurers will accept a deposit premium of 75% at renewal. Please contact us to discuss the various ways we can help.

## PUBLIC & PRODUCTS LIABILITY INCLUDING STATUTORY & EMPLOYERS LIABILITY

For a claim to be paid the occurrence has to happen during the period of insurance. Examples where you might be considered to be liable are a pipe burst in your premises which flooded a neighbour; a fire started in your premises and damaged the building owner’s premises; someone slipped while walking through the car park for which you are responsible. If you did not have liability insurance in place you would have to defend the action against yourself.

Fundamentally, insurers calculate their premium by business occupation/activities, annual turnover and employee numbers and therefore, where there has been a reduction in these aspects, we may be able to obtain a premium adjustment.

## LAID UP VEHICLES, FLEET MOTOR VEHICLES & MOBILE PLANT

Premium reduction options may be available on a case by case basis for laid up vehicles or equipment. The level of premium relief will relate to the reduction in exposure. The majority of insurers are committed to finding the appropriate solution for our clients.

## HOME, CONTENTS & PRIVATE MOTOR INSURANCES

Most insurers will offer generous discounts if you are prepared to accept more of the risk. For example, a \$1,000 or \$2,500 excess removes the insurer’s exposure to small working losses such a crack in window, broken ornament etc.

## TEMPORARY REMOVAL

Generally insurers are providing cover for any property removed from a commercial premises to an employee's property to allow an employee to work from home. However, each insurer has their own guidelines and we need to review your unique circumstances.

## UNOCCUPIED BUILDINGS

Properties which have been vacated solely due to Covid-19 pandemic will continue to be insured for a reasonable period of time. However, each insurer has their own guidelines and we need to review your unique circumstances.

## CESSATION OF WORK

This exclusion has generally been extended to 60 days plus or has been removed during lockdown. However, each insurer has their own guidelines and we need to review your unique circumstances.

## PROPERTY INSPECTIONS

There is a varying approach to the requirement for property inspections but generally insurers have suspended this requirement during Level 4 alert and will await guidance from the NZ Government. However, each insurer has their own guidelines and we need to review your unique circumstances.

## PREVENT A CYBER ATTACK WHILE WORKING REMOTELY – 7 TOP TIPS

With a rapid increase in telecommuting, every device, email server and Wi-Fi network accessed outside the business network is a new potential access point or vulnerability for hackers to exploit. Business leaders must establish strict policies and employee guidelines to ensure that we don't have a cybercrime crisis during this unprecedented push to work remotely. Follow these seven tips to reduce threats.

1. Issue security policy guidance and rules - Annual trainings and email reminders from the IT department are not enough to keep good cyber habits top of mind for employees. A fresh reminder can go a long way to reinforce security best practices.
2. Set up a VPN - a VPN system creates an encrypted tunnel that your internet traffic travels through so it can't be seen by third parties. Setting up a virtual private network (VPN) can seem daunting but just requires a couple hours to configure and isn't technically difficult. VPN with multi-factor authentication should be used as it is the strongest defence.
3. Require Use of Encryption and Wi-Fi Protected Access (WPA) to Secure Networks - while no Wi-Fi is totally secure, private, password protected networks are significantly more secure than public Wi-Fi networks - especially those offered in cafes, hotels and other public places. You can always ask a business that offers public Wi-Fi if private password protected networks are available.
4. Password-Protect Devices Used by Employees and Third Parties - Require employees to use strong passwords that contain letters, numbers and special characters. Avoid using the same password on multiple devices/accounts.

5. Maintain Anti-Virus and Anti-Malware Software - remind employees to install and regularly update adequate security software on all electronic devices they use to perform work remotely. That can be a phone, tablet, laptop, etc. Some employers are eliminating BYOD options and mandating that employees use only employer-supplied equipment and devices.
6. Power Down - encourage employees to power down computers when not in use. Powered off computers are not accessible or susceptible to attacks or intrusions from the internet.
7. Back Up Data - regularly backup sensitive information and, depending on the importance of the data, make sure it is encrypted. Secure backups are the best strategy to prevent critical business disruptions in case of a ransomware attack.

Please do not hesitate to contact us if you have any questions at all.

#### **Acknowledgments**

- a. Cyber - This article belongs to CyberScout and is for informational purposes only. All views expressed do not necessarily reflect the official policy or position of DUAL New Zealand. DUAL New Zealand is not responsible for the content of any third-party website to which links are provided from CyberScout.
- b. Extracts from Professor Allan Manning's Blogs.

*This newsletter is not intended to be specific advice for you and your business and is a general overview of the current environment and how insurance may or may not be affected. In all circumstances, please refer to your Policy Wording carefully and contact your PSC Connect Member Broker for more information*