



# McCormick Harris

## INSURANCE

ADVICE • SOLUTIONS • SERVICE

SPRING 2024

CLIENT NEWSLETTER

## Cyber lessons from the CrowdStrike failure



In July this year, the CrowdStrike outage disrupted businesses around the world. What started as a simple software update quickly turned into a global problem, with millions of systems crashing due to an unexpected error. It wasn't a cyberattack, but the impact was just as devastating. This incident is a perfect reminder for businesses: cyber risks come in many forms, and it's not just hackers you need to worry about.

For many businesses, the immediate focus is on defending against attacks, but what happens when a trusted service provider has an issue like the one CrowdStrike faced? Systems go down, operations halt and, for many, the losses pile up fast. In the CrowdStrike outage, some businesses found themselves unprepared, and those without comprehensive cyber insurance were left to absorb the full cost of downtime, repairs and lost revenue.

According to the Insurance Council of Australia, only about 20% of the nation's SMEs have cyber insurance, leaving many

with no protection from malicious threats and unexpected technical failures that can have equally severe consequences.

Many businesses assume other policies will cover certain digital risks, but this is often not the case.

General liability insurance usually covers bodily injury or property damage caused by the business' operations, products or services. It doesn't cover data breaches, network failures or cyberattacks. Property insurance covers physical assets such as buildings and equipment but generally doesn't extend to intangible assets such as data or digital infrastructure. Professional indemnity (or errors and omissions) insurance may cover claims arising from mistakes in the professional services a business provides, but it usually won't include cybersecurity events such as breaches or hacks unless specifically included.

Cyber insurance policies, on the other hand, protect against:

- Data breach costs: notifying customers,

legal fees and credit monitoring services.

- Cyber extortion: ransom payments and the costs associated with resolving the attack.
- Business interruption: lost income during downtime, including the cost of restoring systems and data.
- Incident response costs: access to cybersecurity experts who help businesses respond to and mitigate the impacts of a cyber event.
- Fines and penalties: fines for failing to protect customer data (such as under the General Data Protection Regulation).

Choosing the right policy can be tricky. It's hard to know what risks you should be covering and how to balance cost against the level of protection your business needs. Your insurance broker can help assess your specific risks – whether it's ensuring coverage for system downtime or providing for legal costs – and help you select a policy that offers real protection for your business.

# Are you unknowingly exposing your business to risk?

Every business deals with contracts, whether it's with suppliers, clients or service providers. But how often do you stop to consider the liability you're taking on when signing those agreements? For many businesses, contractual liability remains an area of risk that is overlooked until something goes wrong. And by then, it's often too late.

At its core, contractual liability refers to the legal responsibility a business assumes under the terms of a contract. This could be anything from agreeing to indemnify another party for certain types of damage to accepting responsibility for delays or defects in a service or product. While some liability is unavoidable in any agreement, businesses need to be aware just how much risk they're taking on – and ensure the contract terms are balanced.

Take a common scenario: a small business signs a contract with a larger supplier. The contract contains an indemnity clause, holding the small business liable for damages caused during the delivery of the supplier's products. If the clause isn't properly reviewed or negotiated, the small business may find itself facing large costs if something goes wrong, even if the fault doesn't lie with it.

Contractual liability coverage helps businesses protect themselves from the financial risks associated with assuming responsibility for certain liabilities. These can include indemnification clauses, damages or losses the business agrees to cover under the terms of an agreement.

General liability insurance usually covers

injury or property damage but may not extend to certain risks you agree to in a contract. Contractual liability insurance is designed to bridge that gap.

Companies must be aware that not all business insurance policies automatically cover contractual liability. You should review your contracts and consult your broker, who can help assess whether your current insurance adequately covers the risks you're assuming under your agreements or if additional coverage is necessary.

Contract negotiations can be complex, but understanding your exposure and having the right coverage in place helps safeguard your financial stability, allowing you to confidently enter agreements while knowing you're fully protected.







# Get ready for natural disaster season

As spring sets in, it is time for a reminder that natural disaster season is approaching.

In November, cyclone season begins in northern regions, and with La Nina still in the picture there is an increased risk of floods nationwide, particularly in already vulnerable regions.

Over the years, we have seen how floods can damage infrastructure, disrupt supply chains and halt operations. Disaster planning is essential.

Meanwhile, the threat of bushfires is ever-present. Climate change has extended the fire season, making the danger more widespread and unpredictable.

So, what can businesses do to prepare? Insurance is one half of the equation. Preparedness is the other.

Start with a risk assessment. Understand how vulnerable your business is to floods,

fires or other extreme weather events. This means looking at your physical location and the broader supply chain. Identify weak points that could cause disruption, whether that's exposure to fire-prone areas, flood-prone infrastructure or reliance on suppliers in high-risk zones.

Businesses in flood-prone areas should check their premises are protected with flood barriers, and ensure drainage systems are maintained and key assets are stored above potential flood levels.

Those facing bushfire risks can reduce hazards by keeping vegetation clear of buildings, installing firebreaks and ensuring equipment such as hoses and extinguishers is in good working condition.

Next, focus on your business continuity plan. Disasters can hit any time, so having a detailed plan ensures you can respond swiftly. It should include procedures for evacuation, communication with staff and

clients, and ways to maintain operations remotely if access to your physical location is restricted. Regularly review and test your plan to ensure it is up to date and that all employees are familiar with their roles.

Keep an eye on weather forecasts and subscribe to local emergency alert systems for timely updates on risks. Early warnings give you the time to activate your emergency plans and protect your business.

Financial preparedness is just as important. Review your insurance to ensure it adequately protects you against the costs of natural disasters. Speak to your broker to navigate this process, identify coverage gaps and advise on the most suitable policies for your situation.

By acting early and ensuring your business is fully prepared, you can mitigate the risks and ensure you're ready for whatever the season brings.



# Is your claims process ready for the unexpected?

When a major incident hits your business – whether it's property damage from a fire or storm, or another unexpected event – the claims process can feel overwhelming. In the immediate aftermath, you are going to have a host of concerns. "How much damage has been done? Is everyone safe? What do I need to do next? Who do I need to contact?"

On top of that, you're probably thinking about how long operations will be disrupted and what this will cost your business in terms of time and money.

After ensuring everyone's safety, the first and most important step is to notify your broker or insurer as soon as possible. Early notification gets the claims process started, and your broker or insurer can then guide you through what needs to be done next.

Before any clean-up or temporary repairs are made, take photos and videos of the damage. Whether it's fire-damaged equipment, water-soaked infrastructure or storm debris, visual evidence from multiple angles will help substantiate your

claim and clearly illustrate the extent of the damage. Follow this by creating a written log, documenting the time and date of the incident, any actions you took immediately thereafter and details of conversations with emergency services or contractors.

Another important step is compiling a detailed inventory of everything that has been damaged. This includes structural components, machinery, stock or furniture. Where possible, include descriptions, estimated values and supporting documents such as receipts or warranties.

If you need to make temporary repairs to secure the premises or prevent further damage, make sure to document every step.

Before-and-after photos and receipts for all work done are essential, as these temporary actions may be included in your claim. Always check with your broker before starting repairs to ensure they meet the requirements of your policy.

Throughout the claims process, keep in touch with your broker or insurer. Keeping

a diary of all interactions – who you spoke to, what was discussed and any agreements made – will also help you stay organised and track the progress of your claim. This simple step can prevent delays and ensure nothing is overlooked.

There are also steps you can take before an incident even occurs. Look at your risk management plan and introduce a proactive documentation strategy. Keep an up-to-date inventory of business assets, maintain records of significant repairs or upgrades, and regularly review your insurance policies with your broker.

These records will allow you to verify the value of lost or damaged items and help your broker accurately assess your needs when reviewing your cover.

Having clear documentation on the state of your business and assets will speed up the claims process if disaster strikes. When your insurer can see that your records are complete and up to date, there's less room for discrepancies or delays.



AFSL number: 238979

**McCormick  
Harris**  
INSURANCE

ADVICE • SOLUTIONS • SERVICE

Toll free: 1300 769 599  
Sydney: 1300 769 599  
Bendigo: 03 5438 1666

Melbourne: 03 8643 4333  
Brisbane: 1300 769 599  
Gold Coast: 1300 769 599

E: [client.service@mhi.com.au](mailto:client.service@mhi.com.au) | [www.mccormickharris.com.au](http://www.mccormickharris.com.au)

For information on our Privacy Policy please head to our website: [www.mccormickharris.com.au](http://www.mccormickharris.com.au)