AIS Liaison
The AIS Insurance Brokers Newsletter
SPRING 2014

Don't get burned this summer

Relaxing in the sun: but how's your business?

Australian summers are not all sunshine, surf and happy holidays. For the unprepared they can be utterly unforgiving.

From bushfires in the south to cyclones in the tropical north, our nation's extreme climate shows its true colours during the summer months.

But even if your company is situated in the central business district or the suburbs, the lessons learned in large-scale disasters still apply – be prepared.

So before you head off for that well-earned holiday, make sure your business is safe and secure.

The Bushfire and Natural Hazards Co-operative Research Centre says last year's exceptional temperatures and low rainfall have contributed to an outlook showing above normal danger for large parts of the country.

Even If you're not in a catastrophe-prone area, vigilance is vital. Remember that even in a "normal" fire season, devastating blazes can still occur.

Bushfires have caused billions of dollars of damage and insurance losses of more than $1.5 billion over the past decade.

And it's not going to get any easier. Thanks to climate change, bushfire seasons are expected to start earlier and last longer.

It's also worth remembering that many – probably most – business losses occur in isolated incidents, not in full-scale civil catastrophes like bushfires or floods.

The summer holiday period is one where many businesses are running at a reduced rate or are completely closed down. Even when the activity level is low, loss can still be caused by a large variety of causes – anything from an electrical fire to a burglary.

So do you have the means to keep your business running if your premises is damaged or burgled? While insurance is a prime consideration when considering the risks your company faces, you can do a lot yourself to eliminate the hazards.

So check your building structures and utilities for weaknesses. Now's the time to fix that leaking washer, flickering electrical connection or rusted-out roofing iron. Loose items left lying around the place should be secured.

In the office, data should be backed up and critical documentation stored safely – off the premises.

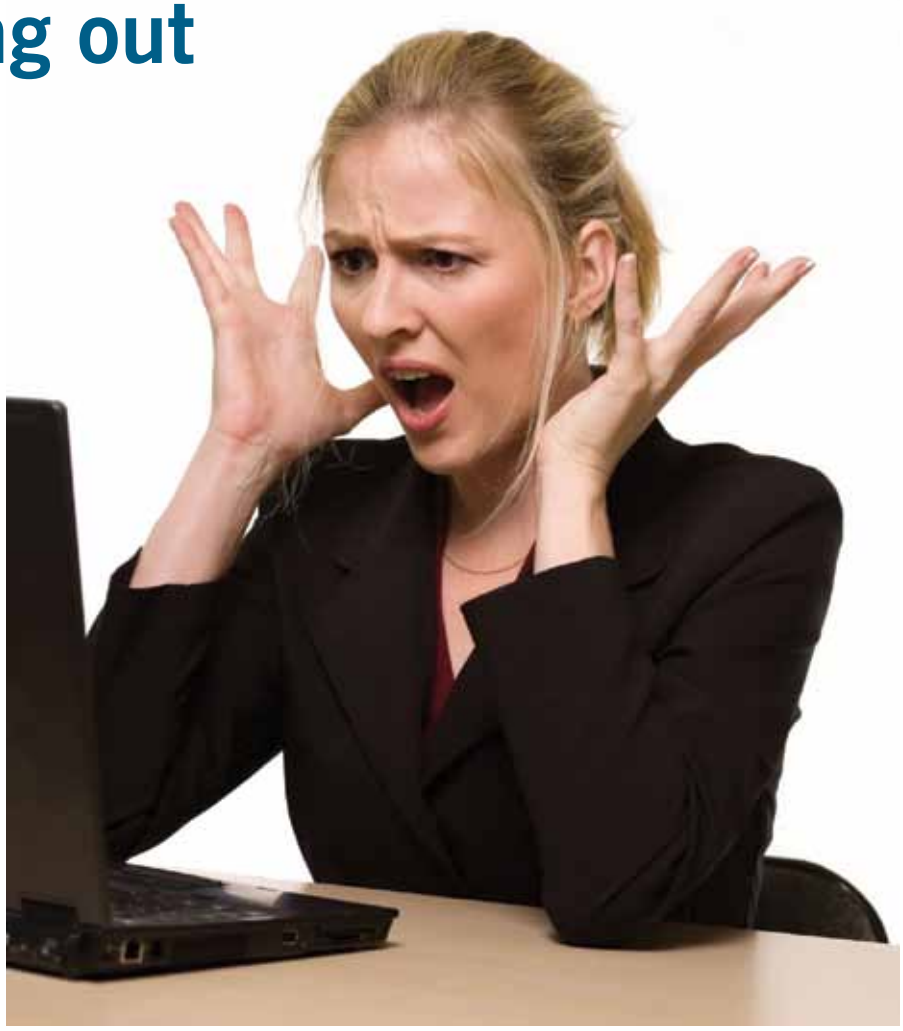
Clear vegetation from around your premises and store flammable materials well away from buildings.

And get your staff involved to make sure you've covered all the bases. The rule is – act now.

Be aware of your level of insurance cover and any exclusions that may apply. That's where we come in.

As summer approaches, there has never been a better time to talk to us about your risks and how we can help give you peace of mind. After all, isn't that what summer holidays are all about?

Take the sting out of a hacking



I've been hacked! Insurers have developed policies to help your business recover

A few years ago the threat of your company being "hacked" seemed a worrying but remote possibility. Today governments and business are waging an all-out war on what has become known as cyber crime, and the possibility of any of us being affected by it has gone from "remote" to "very possible".

Stories of competitors accessing our data and foreign gangsters holding our data to ransom are becoming commonplace. But even as the dangers to businesses stack up, so too do the remedies available.

Last year was dubbed "year of the mega data breach" by IT security company Symantec, which says the number of attacks on SMEs grew 50% on the previous year, accounting for 61% of all cases.

Global figures from business consultants PricewaterhouseCoopers (PWC) are equally stark.

They say the number of cyber-related security incidents increased 48% to 42.8 million last year, with the average loss from breaches growing 34% to $US2.7 million.

Major attacks include one on US retailer Target late last year, when a hacker stole the details of 40 million credit and debit card accounts via malware installed on point-of-sale systems. The criminal also stole the personal details of up to 70 million customers.

Target incurred $US88 million of expenses, including business interruption, reputational damage, data recovery, system upgrades and legal claims.

Its insurance recoveries were $US52 million.

These are huge, headline-grabbing sums – but increasingly it is SMEs that must beware.

"Mid-tier companies are now the weak link and are coming in for increased attention from cyber criminals, because larger organisations have implemented more effective security measures," PWC Australia National Cyber Leader Steve Ingram says.

Rapidly growing threats, according to Symantec, include mobile "malware" that is downloaded via rogue apps, and "ransomware", which locks files and software until a fee is paid to the criminals responsible.

In Australia, cyber crime has been estimated to cost businesses about $4.5 billion a year.

New privacy laws that took effect in March have brought greater scrutiny and corporate penalties of up to $1.7 million, potentially raising the stakes for business.

But while many companies acknowledge the dangers and have taken steps to prevent them, their recovery response has been patchy – according to a recent survey by Zurich Insurance Group and IT consultants Advisen.

They say less than a third of Asia-Pacific respondents have insurance as part of their cyber risk strategies.

As technologies such as cloud computing continue to grow, and as more light is shed on new threats such as government spy agencies, so the cyber-insurance market is expanding and evolving.

Insurers were initially slow to respond with insurance products that covered businesses against the damage that cyber crime could wreak. But a range of policies is now available, tailored to the needs of most types of business. If you're worried about how cyber crime could affect your reputation, steal your data and force you to pay compensation, give us a call.

When products turn into liabilities

Here's a question: What do Kmart apple cutters, Forza scooters, cotton baby pyjamas, Golden Circle canned beetroot slices, Toys 'R' Us toasters and Big W Belgian chocolate have in common?

The answer – they're among the dozens of products that have been subject to recalls in the past couple of months.

And that's just the tip of the iceberg. Around 60 different items, of staggering variety, are currently on the Australian Competition and Consumer Commission (ACCC) recall list.

What this illustrates – besides the fact that danger can lurk in the most unexpected of places – is that every business, large or small, that sells, supplies or distributes goods should have product liability insurance in place.

That applies equally to businesses that don't see themselves as being in the firing line when it comes to product recalls.

Product liability will protect you and your business if you are liable to pay for personal injury or property damages to third parties, and will help minimise risk to finances and reputation.

The policy will cover compensation and the cost of legal proceedings.

Consumers in Australia can take manufacturers to court if they suffer loss or damage due to defective goods. The court will decide if the item was in fact defective, and if so what the level of compensation should be.

Claims can run into millions of dollars and they are more common as customers become increasingly aware of their rights and the variety of products available in Australia grows.

Importers of products can be held liable in the same way as manufacturers. Retailers may also be deemed liable if they cannot identify the manufacturer or importer.

Consumers have three years from the discovery of the defect to bring an action, and the ACCC has the power to bring a case on consumers' behalf, usually when a defect has caused widespread problems.

And if your products were recalled, could your business survive?

Identifying who you sold the products to or where the unsold products are in your stock system and recovering them could result in enormous costs – plus the impact on your business reputation could be devastating.

With product recall insurance, recall costs are recoverable and some policies give advance payments.

Businesses of all sizes – any business that sells something to the public – should foster a culture of safety, with proper design, production, record-keeping and marketing procedures and a quality assurance system in place.

Above all, arrange appropriate insurance cover. There are enough risks in business without taking unnecessary chances.

Who could have foreseen the apple cutter blade could detach, potentially causing lacerations, or that the beetroot slices contained "microbial growth", or that the plastic toast in the child's toaster could crack into choke-size pieces?

Don't just assume she'll be right. Chances are, at some point, she won't.

Talk to us to find the policy that suits your business needs, and plan for the future with confidence.

It has to be safe: product liability insurance protects businesses in an increasingly challenging sales environment

Hashtags and hash-ups

The emergence of social media such as Facebook and Twitter have created a host of marketing opportunities and given SMEs unparalleled access to their customers and clients.

Their uses include targeted promotions and one-on-one dialogue, recruitment, data collection and customer profiling, and crowdsourcing of ideas and opinions.

However, for every plus there is a potential minus, and businesses that fail to mitigate their risks could pay a heavy price.

According to a recent report by business advisers Grant Thornton, threats from social media fall into four broad categories.

The first and most common is damage to reputation, which can result from ill-judged posts, rogue comments from disgruntled staff or negative reviews and reactions among consumers.

Unfortunately, people are much more likely to share their bad experiences than their good ones, and what may seem like an ideal opportunity to engage with the public can soon turn sour.

Once a Twitter or Facebook "fail" goes viral, it can soon blow out into a public relations disaster.

JP Morgan learned this the hard way late last year when a live question-and-answer session on Twitter devolved into a series of abusive posts pointing out the finance giant's perceived lack of ethics.

The other threats raised by Grant Thornton are disclosure of confidential information, such as loss of private customer data either accidentally or through hacking; legal breaches, including defamation and copyright; and corporate identity theft – such as when Burger King in the US had its Twitter feed hijacked by a prankster who posted offensive tweets and changed the company's logo to that of rival McDonald's.

NSW District Court judge Judith Gibson told a recent Australian professional indemnity conference that employee misuse of social media is a major danger.

"The potential for business losses arising from use or misuse of social media is enormous," she said.

Justice Gibson says it is essential to develop a clear staff social media policy.

The Grant Thornton report says best practice for controlling social media risks includes a detailed risk analysis; a governance structure with clear roles and responsibilities – with senior, qualified figures taking responsibility for social media use; close monitoring of posts across all platforms; and regular training for staff on policies and usage.

The internet is a fast-moving environment, with opportunities and threats developing all the time, but insurers are working to keep pace, as evidenced by the growth of cyber cover.

Feel free to contact us to discuss the ways you can protect yourself against the consequences of a social media policy that goes wrong.

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