**5 reasons why your company needs cyber insurance and how to get it**

The reality is that your company is almost certain to experience a cyber security incident, such as a data breach or [ransomware](http://blog.ajg.com.au/blog/2017-the-year-of-the-ransomware-epidemic) attack. And without the proper risk management strategies and insurance policies in place, such an attack could seriously threaten your financial viability and ability to do business.

Still not convinced you need cyber insurance? Here are 5 reasons why you do.

**1. Your staff rely on computers to get their jobs done**

We hate to state the obvious, but here’s the thing: if your organization uses any internet-connected devices for work purposes, you need cyber insurance.

Simply accessing the internet on devices – whether they be computers or smartphones on or off your network – **puts your business at risk** of a cyberattack.

 **The bottom line? Nobody is immune to cyber risk,** and every company that’s using technology and the internet needs cyber insurance as part of an effective risk management plan.

**2. Your company handles and/or stores personal data from clients and customers**

If you use, store or disclose **personal information** about your customers or clients, you need cyber insurance. Why? Because this information is a [valuable commodity](http://www.zdnet.com/article/hackers-dont-just-want-your-credit-cards-now-they-want-the-pattern-of-your-life/) for hackers, and collecting it makes you a target for **data breaches** and other cyber security incidents.

Personal information refers to any information that can be used to ascertain or reveal someone’s identity such as their name, address, email address or telephone number. In accordance with the [Privacy Act](https://www.oaic.gov.au/privacy-law/privacy-act/) it’s your responsibility to ensure that this type of information is collected, used and stored in a **safe** and **compliant** manner. In addition to being aware of your [privacy obligations](https://www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-20), you need to mitigate your cyber risk exposures with a risk management program, cyber insurance and a **data breach**[**response plan**](http://blog.ajg.com.au/blog/what-will-mandatory-data-breach-notification-mean-for-your-business).

Data breaches are an [increasingly common](http://www.computerweekly.com/feature/The-true-cost-of-a-cyber-security-breach-in-Australia). It’s worth noting that the organization considers this number to be lower than the *total* number of cyber security incidents affecting private companies; the true extent of cyber incidents is unknown.

**So here’s the key takeaway: handling personal information is a cyber risk exposure that you need to mitigate with risk management and cyber insurance.**

**3. You use cloud services**

It’s safe to say that cloud technology has entered the mainstream of business ICT.

If you’re among the high percentage of cloud-friendly businesses, you need cyber insurance. Here’s why:

* [Research](https://www.skyhighnetworks.com/cloud-security-blog/12-must-know-statistics-on-cloud-usage-in-the-enterprise/) has shown that 2.7% of files shared in the cloud are **publicly accessible**;
* **1%** of files **uploaded** to the cloud contain sensitive data, and 44.4% of this data includes confidential information such as business plans and financial records;
* Personally identifiable information (PII) [accounts for 70%](http://apac.intelsecurity.com/event/wp-content/uploads/sites/2/2016/05/IntelSecurity_ANZ_Privacy-DataSheet-PAW_web.pdf) of date being **stored** in the cloud.

According to [Intel Security](http://apac.intelsecurity.com/event/wp-content/uploads/sites/2/2016/05/IntelSecurity_ANZ_Privacy-DataSheet-PAW_web.pdf), more than a third of Australian businesses don’t have a policy about staff sharing information via the cloud despite widespread cloud adoption and concerns about data breaches. **So take note: the cloud is a great tool for file sharing and collaboration, but without proper governance and cyber insurance, it exposes your business to a data breach.**

**4. Your business couldn’t financially survive a cyber attack**

Quantifying the cost of a cyber-attack is difficult, but estimates range from [between $200,000](https://www.staysmartonline.gov.au/sites/g/files/net301/f/Cost%20of%20cybercrime_INFOGRAPHIC_WEB_published_08102015.pdf) and [over $600,000](https://www.staysmartonline.gov.au/sites/g/files/net301/f/Cost%20of%20cybercrime_INFOGRAPHIC_WEB_published_08102015.pdf) per incident – high enough to certainly cripple a small business.

But these estimates don’t account for the indirect, hidden costs of a cyber-attack which includes (but isn’t limited to):

* Business interruption or destruction
* Reputational damage and loss of customer trust
* Insurance premium increases
* Lost contract revenue and loss of IP
* Damage to share price

When we take these kinds of *indirect* costs into account, the total cost of a data breach skyrockets:

**A cyber-attack could seriously compromise your financial viability**, so must have a cyber insurance policy in place. At the very least, this will cover risks such as financial loss arising from lost revenue, customer churn, privacy fines and legal expenses. Learn more [here](http://arthur-j-gallagher.s3.amazonaws.com/downloads/1211-ajg_cyber_infographic_july_2016.pdf).

**5. Your existing insurance policies may not cover losses from a cyber attack**

Some general business liability policies include cover for cyber liability, but many don’t.

Don’t assume that you’re covered just because you have [public liability](https://techcrunch.com/2016/06/13/cyber-insurance-is-changing-the-way-we-look-at-risk/), management liability or other business insurance policies in place. You need a separate [cyber insurance policy](https://ajg.com.au/insurance-solutions/cyber-insurance?__hstc=76516298.5817fdb3ee36081a2c2ab590f2bbbeca.1496823281492.1496823281492.1497310476084.2&__hssc=76516298.3.1497310476084&__hsfp=3339848637) that covers your risk exposures and, at the very least, includes cover for things like business interruption, loss of data, legal expenses and data recovery.

**Cyber Liability Coverage** is obtainable through a commercial insurance agency. Your broker can help to assess your company’s exposure to find the policy that suits your unique needs best.

Patti Buell, Broker

Insurance Risk Advisory Group

727-277-7363