Cyber Roadblocks
Five Common Misconceptions

What is Cyber Liability & Privacy Protection and who should buy it?

Cyber Liability & Privacy Protection insurance is designed to address the exposures Insureds face when using the internet, email, websites, computer programs and in particular, from storing private information about their clients.

We often hear that clients don't buy a Cyber Liability & Privacy Protection policy because they don't think they have an exposure, or because it won't happen to them, so we have put together some talking points to combat those common misconceptions.

1

I don't hold valuable data

Valuable data isn't limited to intellectual property. It can be as simple as your employees', suppliers', and even your own personal details such as full name, date of birth, drivers licence number, Tax File Numbers and bank account details.

Most businesses will hold this information about their employees or suppliers as a minimum, meaning they are at a higher risk of being targeted for a cyber-attack.

If a cyber-attack were to occur and this valuable data stolen, it may be used by an attacker to commit identity fraud (such as taking out a loan in someone else's name) or as the basis for a social engineering or phishing attack.

When this happens, an Insured may have to notify the Office of the Australian Information Commissioner (OAIC) (previously known as the Privacy Commissioner) as well as the individuals affected by the attack, that this information has been stolen. In this instance, an Insured may need to refer all affected individuals to a Credit Monitoring Facility. This will alert the individual when a line of credit has been requested to be opened in their name. An Insured may also incur legal fees to identify whether the attack meets the definition of a breach of privacy under legislation based on the type of information exfiltrated. Panel lawyers may also represent the Insured in claims made by affected individuals brought against them as a result of the breach. Additionally, the Insured may be liable to receive a fine from the Information Commissioner.

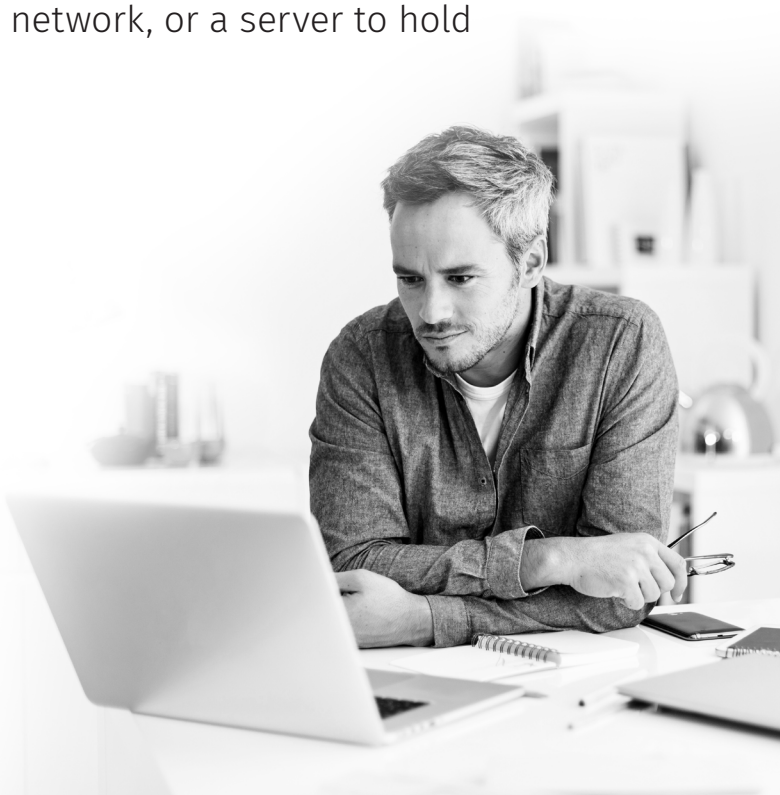
2 I don't transact online

An Insured's business may not have a website, however most businesses use a computer, a local network, or a server to hold electronic files and records.

A business may also do their banking online, or manage their invoicing, both of which may include sending and receiving personal or sensitive information. An Insured may also receive supplier invoices via email which can be easily accessed in the case of a system breach or cyber-attack.

According to a recent report from the OAIC, 35% of data breaches are the result of human error. For example, an employee may unknowingly forward an email containing malicious software. They may also accidentally send valuable and sensitive data to an unintended recipient.

The OAIC also notes that 59% of data breaches are malicious (criminal) via phishing, hacking, or deliberate malware attacks which only require an internet connection for a hacker to access an inadequately protected system.



3 Our data is safe in the Cloud

Did you know that an Insured is legally responsible for the information that is stored in their cloud, even if a hacker accesses the cloud via a third party?

A common example of this is an Insured's outsourced IT provider. As a result of this, an Insured may incur notification costs (to both the OAIC and the affected individuals), remediation costs and legal costs.

Data stored in the cloud can be accessed, copied, stolen or altered just as easily as data stored on a computer or a server. Once a breach occurs, the information in the cloud is still classified as 'breached' even though there may be multiple soft copy backups that mirror the information stored in the cloud. Even though the sensitive information has not been lost, it has been accessed by an unauthorised party, and is still subject to the relevant privacy legislation.

Depending on where a cloud provider is located, varying laws from different jurisdictions around the world may apply to the information held. In this instance, lawyers will need to identify which countries' laws apply to which breach, and what breaches of that law have occurred. It doesn't take many competing jurisdictions for this to add up to a very expensive exercise. Depending on the law that applies to the potential breach, there may also be significant fines and penalties against the Insured as a result.

4 Our IT employee / IT consultant will take care of it

Does your IT employee or IT consultant work 24/7? A Cyber Liability and Privacy Protection Policy offers 24/7 emergency Incident Response services.

Does your IT employee or IT consultant have the necessary IT forensic skills and qualifications to investigate this type of incident? A Cyber Incident Response Team is made up of individuals who have the experience and global expertise in these fields to help mitigate further loss, mediate complicated situations, and provide the best advice on what action to take next.

5 Our IT system cannot be breached

No system can be 100% safe.

The world's most secure systems have been breached – i.e. FBI, Commonwealth Bank of Australia, Facebook and Sony. As these large corporations, who have the budget for high tech cyber security, are able to be hacked, then it is more than likely that a hacker will be able to hack an SME company. Criminals see these SME companies as quick and easy money given the low security measures in place.

Given the need for security, software developers are constantly issuing 'patches' to help reduce the number of hacks, however these may not necessarily help in all cases.

The OAIC has advised that 5% of breaches have resulted from a system error. This includes mobile phones, tablets or laptops being misplaced or lost in public places and in the event that these devices aren't encrypted, they can be easily hacked. Should this happen, an Insured may be required to notify the OAIC and affected individuals, which can involve significant legal costs which may not be budgeted for due to the belief they are adequately protected against cyber and privacy breaches.

We hope the above information assists in considering these common misconceptions in the market.

DUAL's WebRater Cyber Product Suite

is made up of two offerings targeted towards the SME market.

- Cyber Platinum is DUAL's original Cyber offering and is aimed towards SME clients with up to $50M turnover.
- Cyber Gold is designed for the micro SME market, consisting of clients with up to $5M turnover.
- For larger clients, please contact your local DUAL Underwriter to discuss.

Cyber Gold

Cyber Platinum

Find out more

For further details on our Cyber product suite, please contact your local DUAL Underwriter.