Business cyber security obligations.

Cyber-attacks are a constant threat to individuals and businesses. From malware to phishing, cyber security risks are on the rise and attacks are becoming more sophisticated. While you may think your business is safe and you have done everything to protect it from a security breach, the truth is no system is impenetrable.

Large corporations with up to date software and protections in place have fallen victim to cyber-attacks. There have been successful attacks, both within Australia and internationally, on a range of organisations such as financial, IT, healthcare and telecommunications as well as governments at various levels.

In comparison, small business owners may assume, or hope, that the information and data they hold would be of little interest to hackers. However, small businesses that hold sensitive data such as healthcare records and credit card information, or vulnerable data such as childcare records, are a target for hackers too. Some small organisations are less advanced in terms of their data security, and this can make them an easier and more realistic target. Gaining access to a small business can also, in some cases, give hackers access to larger corporations.

Protecting your business from a cyber-attack

It's important for all businesses to understand that protecting themselves from a cyber-attack is not just an IT or management issue. This requires a whole business focus that all staff need to be aware of so they can contribute to the risk management processes and systems. If any staff fail to adhere to the strategies put in place, regardless of that staff member's role and level of responsibility, this can put the business at risk.

There are many ways a business can be protected from a cyber-attack. From software updates and data backups to passwords and staff training, the options available are improving all the time.

To find out what you can and should be doing to protect your business, go to **https://www.cyber.gov.au/resources-business-and-government**

Incident response plan

An incident response plan is documented instructions for what to do if your business experiences a cyber-attack. These instructions help minimise the damage and improve the response and recovery time.

The plan should include an outline of what threats could impact your business and a strategy to manage each incident type with clear timelines. The plan should also identify the critical assets that could be a target, such as customer information, so the business knows what it needs to protect.

A list of responsibilities and accountabilities should also be included so that staff are aware of their roles in dealing with the situation. APR or media response plan could also be something you incorporate in case you're required to make public statements regarding the incident.

To find further details search on incident response plans, go to **https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/publications/cyber-incident-response-plan**

Notifiable Data Breach (NDB) scheme

The NDB scheme requires all businesses covered by the Australian Privacy Act 1988 to notify the Office of the Australian Information Commissioner (OAIC) and affected individuals when an eligible data breach has occurred. Businesses covered by the Privacy Act includes all organisations with an annual turnover of more than $3 million. The Privacy Act also covers some small businesses who have an annual turnover under $3 million if they operate in one of the following categories:

- A private health service provider such as a day surgery or a pharmacist
- An allied health professional
- Complimentary therapy such as a naturopath
- A gym or weight loss clinic
- A childcare centre, private school and private tertiary education institution
- A business which sells or purchases personal information

An eligible data breach occurs when:

- there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an organisation holds
- the breach this is likely to result in serious harm to one or more individuals, and
- the organisation or agency hasn't been able to prevent the likely risk of serious harm with remedial action

Serious harm to a person may include serious physical, psychological, emotional, financial or reputational harm. Determining if serious harm is likely, meaning more probable than not, requires as assessment from the perspective of a reasonable person.

A quick response to a data breach decreases the impact of the breach on those affected. To be able to respond quickly, a data breach response plan is needed. This plan will outline the business' strategy for containing, assessing and managing the incident from start to finish.

Further information about the Notifiable Data Breach scheme can be found at **https://www.oaic.gov.au/privacy/notifiable-data-breaches**

Cyber insurance

Cyber insurance can help cover financial losses to your business, your customers and other parties following a cyber security breach. This might include costs associated with:

- Loss of revenue due to interrupted business
- Hiring negotiators and paying ransom
- Recovering or replacing your records or data
- Liability and loss of third-party data
- Defence of legal claims
- Investigation by a government regulator
- Misuse of intellectual property online
- Crisis management and monitoring
- Prevention of further attacks

When considering cyber insurance, it's crucial to choose an insurer who understands cyber risks are changing, and new risks are constantly emerging. The costs of a cyber-attack can be enormous. However, the right insurance policy will help safeguard your business now and well into the future.

Contact Guild Insurance on **1800 810 213** if you are considering taking out cyber insurance and would like further information.