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 continually getting 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.

The Australian Cyber Security Centre's 2016 Cyber Security Study reported that 90% of Australian businesses have experienced a security breach or threat. Even large corporations with up to date software and protections in place have fallen victim to cyber-attacks. There have been successful attacks within large financial institutions, IT and software development companies, governments and large hospitals. Examples include; Uber, Facebook, Ashley Maddison, Australian Red Cross and the Australian Bureau of Statistics to name a few.

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 is a whole business issue 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.

Tips for protecting your business from a cyber-attack

- Be sure staff only have access to what they need; don't grant universal access across a business
- When staff leave the business, remove all access and permissions immediately
- Create strong passwords
- Engage IT security experts to assist with your cyber security
- Train all staff about the risk of a cyber-attack and the prevention strategies in place
- Regularly back up data and information
- Use the resources and information found on **www.staysmartonline.gov.au**

Cyber attacks are the fastest growing crimes throughout Australia and across the world. And with the majority of businesses not insured against cyber attacks, the effect can be crippling.

90% of Australian businesses have experienced a security breach or threat

58% have experienced a successful incident

86% have experienced an unsuccessful attempt

Australian Cyber Security Centre's 2016 Cyber Security Study

Incident response plan

If your business does suffer from a cyber-attack, you need to have a response plan to help minimise the damage as quickly as possible. The Notifiable Data Breach (NDB) scheme also requires you to have an incident response plan; if you're required to report a NDB to the Office of the Australian Information Commissioner (OAIC) then they will also ask about details of your response plan.

The plan should include an outline of what threats could impact your business and a strategy to manage each incident type with clear timelines and objectives. Identify the critical assets that could be a target such as customer information so that you can review if the current incident is beginning to affect other areas of the business.

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

The details of your cyber insurance provider and cover should be noted in case you need assistance or if a claim needs to be lodged. Depending on the details of your insurance product, you may be provided with assistance in dealing with the incident.

You can find further details about what to include in your incident response plan at **www.staysmartonline.gov.au/protect-your-business/recover-when-things-go-wrong/incident-response-plans**

Notifiable Data Breach (NDB) scheme

The NDB scheme commenced on 22 February 2018 and businesses need to be sure they understand their requirements.

The NDB scheme requires all businesses covered by the Australian Privacy Act 1988 to notify the OAIC and affected individuals when a notifiable data breach has occurred. A notifiable data breach is a breach which is considered likely to result in serious harm to individuals that information relates to. This breach may occur when information is lost or has been accessed or disclosed without authorisation.

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

The Guild Cyber Insurance product assists with notifying the OAIC of a notifiable data breach. It can also assist with costs associated with notifying all affected individuals.

Cyber insurance

Cyber insurance is a product that can assist businesses that suffer a cyber-attack. The product can help protect against a range of information technology risks like an IT system breach from hacking or malware, third-party claims and the costs involved with responding to an attack.

The Guild Cyber Insurance product exists to protect you and your business now and into the future. The product includes cover for a range of online threats, business interruption, third-party claims and cyber event response costs.

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.

To obtain a cyber insurance quote contact Guild Insurance on **1800 810 213.**

1800 810 213 **guildinsurance.com.au**

Better through experience.

Guild INSURANCE

Cybercrime

The Australian Cyber Security Centre's 2016 Cyber Security Study found the following:

Cyber attacks are the fastest growing crimes throughout Australia and across the world. And with the majority of businesses not insured against cyber attacks, the effect can be crippling.

90% of Australian businesses have experienced a security breach or threat

58% have experienced a successful incident

86% have experienced an unsuccessful attempt

Of those who've experienced a security breach or threat, the following impacts were reported:

56% required additional staff time to deal with the incident

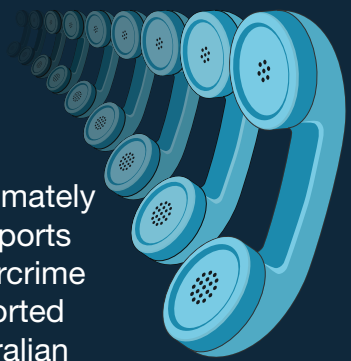
35% had staff prevented from doing their work

39% felt financial impacts, mainly consisting of further investment required to prevent future incidents (33%) or external repair and recovery costs (11%)

Stay Smart Online, an Australian Government program, states that:

The average cost of a cyber-attack to a business

The average time to resolve an attack



Approximately **4000** reports of cybercrime are reported to Australian Cybercrime Online Reporting Network each month

Better through experience.

Guild INSURANCE

Australian Cyber Security Centre's 2016 Cyber Security Study
GLD4415 Risk HQ Article Infographic 02/2018