Debunking cyber myths for SMEs

Preventative measures against imminent cyber-attacks

As an Australian business you have no doubt been bombarded with insurance articles referring to the rising prevalence of cyber threats. On a daily basis the headlines report the names of large organisations that have fallen victim to cyber-attacks such as phishing, hacking, and ransomware like WannaCry. There are endless reports that cyber claims are on the rise, mandatory data breach notification laws are here, and that there are many solutions to protect you. But as an SME are you actually exposed? And is the cost really worth the size of the risk?

The truth is the decision to purchase insurance is yours. By opting out of insurance your organisation is choosing to be accountable for the financial implications of any loss or fine that occurs as a result of a cyber incident – including any interruption to your business. This is known as 'self-insuring'. But are you self-insuring by default, or by choice? And importantly is the decision based on facts, or myths?

This guide is designed to help you understand what self-insuring your cyber risk means and importantly help you make this important decision with confidence.

AON
Empower Results®

DEBUNKING CYBER MYTHS FOR SMES

MYTH #1

"I am not a large business, cyber is just not an exposure for me"

SPYWARE

Hackers are increasingly targeting smaller businesses as their data security tends to be less advanced than that of larger businesses. In *The Small Business Cyber Security Best Practice Guide*[1], the Australian Small Business and Family Enterprise Ombudsman asserts that:

- 43% of cybercrime targets smaller businesses.
- 22% of smaller businesses hit by cyber-attacks are so badly affected they cannot continue operating.
- 60% of smaller businesses that experience a significant cyber breach go out of business within the following six months.

MYTH #2

"My IT guy knows his stuff, he is a guru"

ACTIVE PROTECTION

Firewalls, a quality IT team and antivirus protection are all great strategies around data protection, but they are not the silver bullet.

Ask yourself this, how could companies like Yahoo, JP Morgan Chase, eBay and Target Stores with their large IT teams, and robust IT systems still experience data and security breaches, resulting in significant financial losses into the millions, as well as reputational damage to their business?

MYTH #3

"We don't hold credit card or financial records; we have nothing of use, why would someone want to target my business?"

BUSINESS INTERRUPTION

For an SME, the bigger risk is interruption to your business despite not having such sensitive information. This may include social engineering and cyber extortion.

As an SME you're more likely to have unique product offerings, client information, invoicing and payment records, etc. Essentially, your intellectual property that has been built over years of operation and is key to your success – and is also your asset.

It's not about the data being useful to the hacker; it's how the data and records are useful to your organisation, and importantly, how well (or how long) your business could function without them.

MYTH #4

"I outsource to a Cloud provider"

CLOUD COMPUTING

When outsourcing to a third party (60% of Australian companies use cloud computer services), you don't outsource your liability or responsibilities for the data that is managed externally. You'll still be liable if a breach occurs at your service provider's end. We recommend you discuss this with any third party cloud provider that you may be using.

If your clients are providing you with their information (whether it be corporate information or personal), you have a duty of care, and are responsible for the safety of that information. As a business you should be aware of this as well as your obligations and the potential risks. With the arrival of mandatory data breach notification laws this points to a mounting problem.

MYTH #5

"I am covered under another policy for my cyber exposure"

CYBER INSURANCE

When we consider the speed and complexity of cyber risk and exposures and how they evolve, ask yourself if your conventional insurance policies are evolving at the same pace?

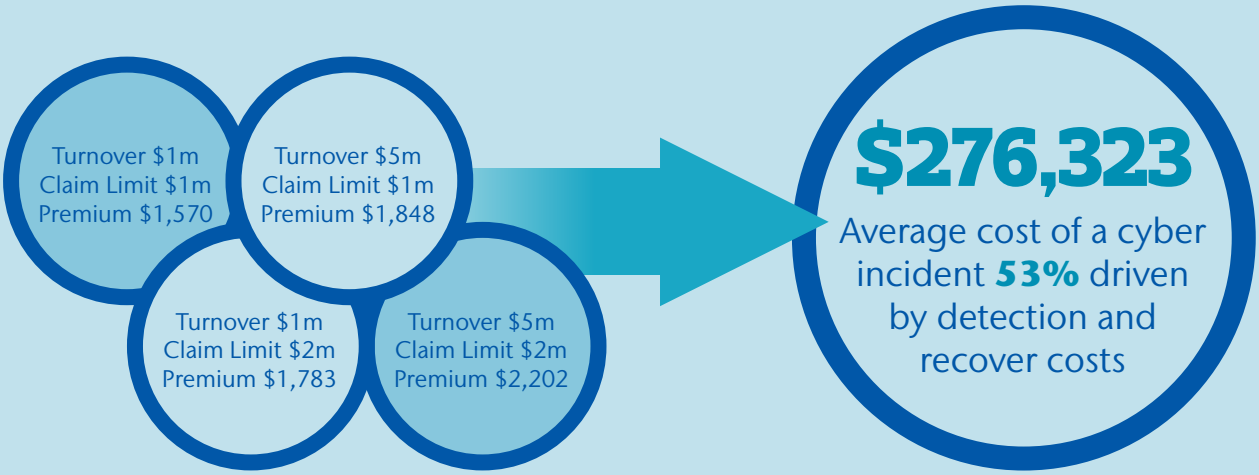
While endorsements are a nice to have, traditional insurance policies were never designed or rated to cover cyber risks and will only ever provide partial cover, if any at all. It's important to do your homework and clarify what's covered and what limitations are associated with it.

PREVENTION IS AN INVESTMENT

The cost of insurance vs self–insurance

With pressure on SMEs to do more with less, it's understandable that the default position for cyber is to finance the potential losses yourself. But how do you assess the feasibility, compare costs and make an informed decision around the best option for your business?

Consider this:



Quoted premiums do not vary for professional, manufacturing or retail industries.

Case study

Even with these preventative measures, however, no organisation is immune, regardless of their size or exposure. In our office alone, we have seen a spike in cyber incidents recently, including:

- A local school had emails forged from a key person in the business with over $130,000 in funds transferred to false accounts.
- A small engineering firm subject to ransomware resulting in business interruption for 3 days.
- An aged care facility experienced a significant data breach resulting in the release of hundreds of personal records.

All of these companies had similar characteristics, they were all SMEs, and none of them had a cyber policy.

NEW DATA BREACH NOTIFICATION LAWS

The resources and money needed to recover from a cyber attack can put a business out of operation for months if not completely. With the introduction of new data breach notification laws - if your business turnover is **$3m** you could be fined $2m or more in the event of a security breach. Businesses that deal with health records, credit data, etc., regardless of revenue are NOT exempt.

References

[1] https://www.asbfeo.gov.au/sites/default/files/documents/ASBFEO-cyber-security-guide.pdf
[2] https://www.staysmartonline.gov.au/sites/g/files/net301/f/Cost%20of%20cybercrime_INFOGRAPHIC_WEB_published_08102015.pdf

3 STEPS TO TACKLE CYBER THREATS

Protect your assets
Invest in good IT support and ensure your website, point-of-sale (POS) systems and software are up to date with the latest updates.

Back up
Ensure you regularly back-up important data and information to reduce the damage in case a breach occurs.

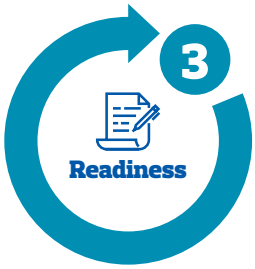
Safe surfing
Browse safe sites, and use applications you trust on company computers, tablets or phones.

Strong passwords
Ensure that you use 'smarter passwords' or even multi-encryption authentication.

Smarter protection
Have clear policies & security measures relating to your systems, data protection and privacy in case a breach occurs. Ensure your business is aware of this.

Awareness is action
Train your staff on the risks and importance of protecting sensitive information. Especially customer information.

On-going education
Provide regular awareness sessions with staff, on how to identify irregular behaviour and how to be vigilant.



Plan ahead
Ensure you have a strong incident response plan and test it regularly.

If you think a breach has occurred inform your insurance provider and relevant authorities to understand what you have to do next.

Conclusion

So the choice continues to be yours, insure or not. But ensure it is an informed decision, and one that is based on answers to questions like:

- Do you have access to resources and funds needed to respond to an incident in a way that it will not impact your operation, your clients or your cash flow?
- If your intellectual property was held for ransom, would you be able to continue without it?
- Are you implementing prevention measures beyond IT security systems such as incident response plans?

aon.com.au/smecyber

AFF0992A 0718

AON
Empower Results®