BlueRock

The Pros and Cons of Cyber Insurance

CompTIA Melbourne Meeting 9th May 2023

Adam Gibbins

Director BlueRock General Insurance

adam.gibbins@thebluerock.com.au

0402 050 557

Australian cyber snapshot

- A cyber attack occurs in Australia every 8 minutes.
- Cyber crime costs Australian business over $1B annually, yet it is one of the least widely insured risks.
- Unisys Security Index Australia 2022 revealed that 15% of Australians would stop dealing with an organisation if their data was breached.
- In 2022 63% of Australian organisations suffered a Cyber security breach.
- Australian SME's are of increasing interest to cyber criminals - it's not just the big internationals at risk.
- The majority of Australian SME's continue to think of cyber as an "IT problem" rather than a board/ownership level risk.

What does cyber insurance cover?

Cyber insurance is designed to provide financial protection in the event of a cyber attack or data breach. The benefits provided by cyber policies vary, but generally may include:

- **Data breach response and investigation costs:** This may include the cost of hiring forensic experts to investigate the breach, notifying affected individuals, credit monitoring, and public relations expenses.

- **Business interruption losses:** Cyber insurance can cover the loss of revenue resulting from a cyber attack, such as a website being taken down or a business being unable to process orders.

- **Cyber extortion & crime:** This coverage can help cover the cost of ransomware payments, negotiations, and legal expenses. Social engineered theft is currently the biggest driver of claim activity.

- **Cyber liability:** This can include the costs of legal defence and settlements or judgments resulting from a data breach or cyber attack.

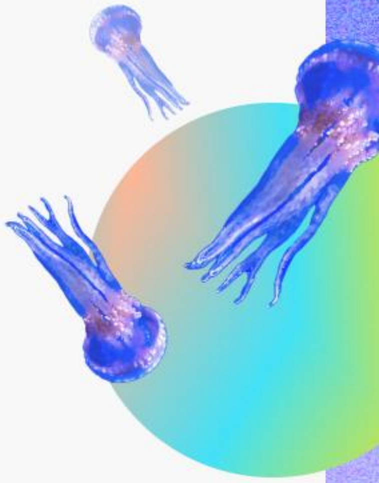
- **Network security liability:** Protect against claims of third-party damages resulting from a cyber attack, such as a virus or malware spreading to a customer's computer or network.

Cyber insurance policies can vary significantly in terms of coverage and cost, so it's essential to review policy details to find the best coverage for your specific needs.

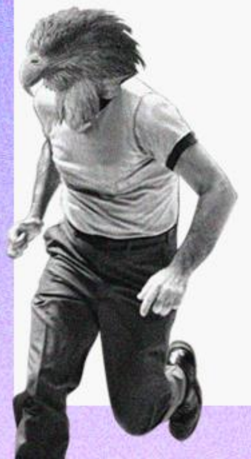
Who needs cyber insurance?

Cyber insurance can be beneficial for businesses that uses technology and store sensitive or confidential data, including:

- **Businesses of all sizes that store sensitive customer data** - credit card information and medical records.
- **Healthcare providers and allied health businesses** - electronic health records.
- **Financial institutions such as banks, credit unions, and investment firms** - sensitive financial information.
- **Online retailers and e-commerce businesses** - customer information, such as addresses and payment details.
- **Educational institutions** such as schools, RTO's, and universities - student information and research data.
- **Any organisation that relies heavily on technology** and may suffer financial losses due to a cyber attack or data breach.



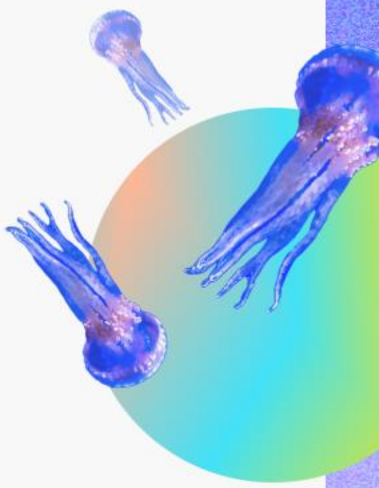
Essentially, any entity that uses technology to collect, store, and process data should consider purchasing cyber insurance to protect against the cost of potential cyber risks and data breaches.

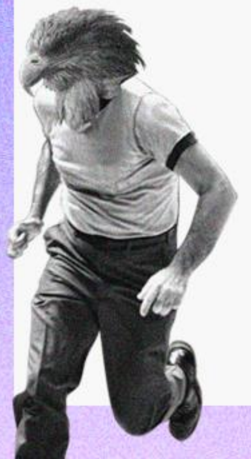


Who needs cyber insurance?

Take a moment to consider:

- The effect to your business if a hacker blocked access to all your files and demanded a hefty ransom for release?
- Could you sustain a complete interruption to your business operations due to a cyber attack?
- Is it possible that you or your staff could fall victim to a fraudulent email releasing personal information or directing funds?
- The effect of a data breach to your business?
- The amount and personal nature of customer data you store and the security arrangements in place to protect that data.





Real cyber claim examples

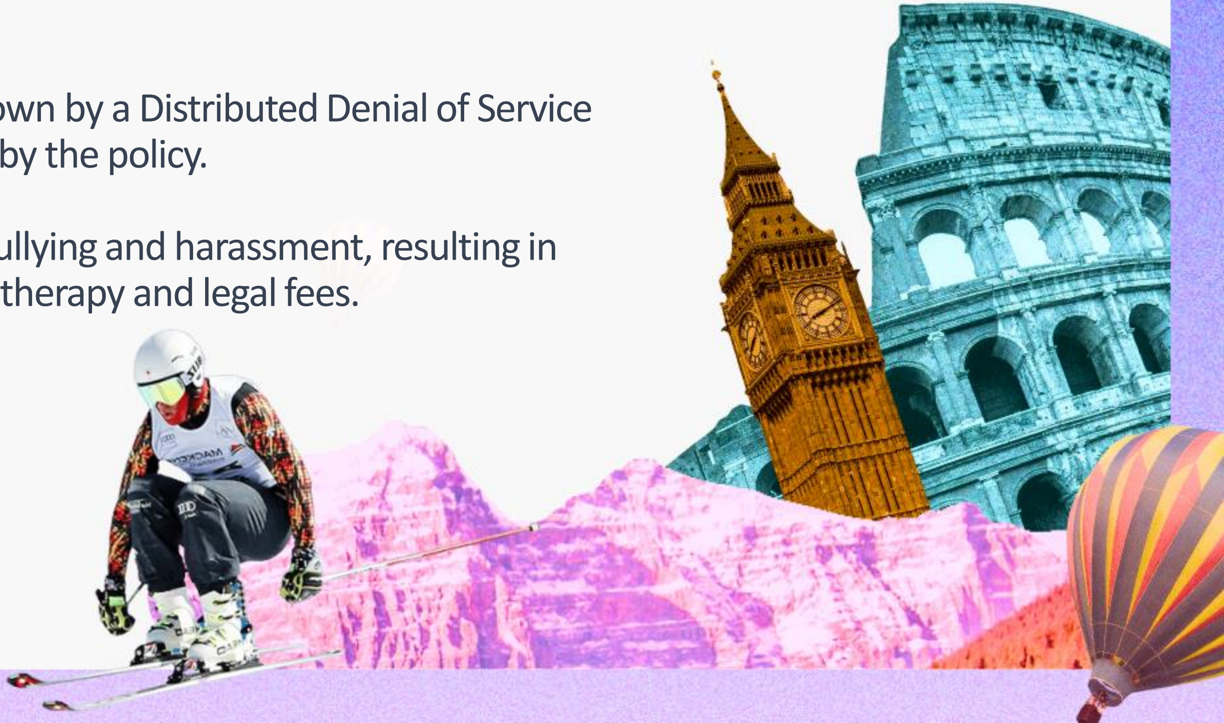
- **Ransomware attack:** A physio clinic’s system was compromised by ransomware, which resulted in the loss of important data. The attacker demanded a ransom payment to release the data. The policy covered the cost of the ransom payment and data recovery.

- **Social engineering attack**: An employee of a share registry firm was tricked into initiating a transfer of funds by a fraudulent email that appeared to be from a client. As a result, the company suffered a loss of funds, which was met by the policy.

- **Data breach:** An online retailers system was hacked, and confidential customer information including credit card details, was stolen. The company incurred significant costs associated with notifying affected customers, providing identity theft protection, and legal expenses. These costs were met by the policy.

- **Business interruption:** A travel services company's website was taken down by a Distributed Denial of Service (DDoS) attack, resulting in an immediate loss of revenue which was met by the policy.

- **Cyberbullying and harassment:** A restaurateur was the victim of cyberbullying and harassment, resulting in emotional distress and loss of reputation. The policy covered the cost of therapy and legal fees.



Considerations when buying cyber insurance

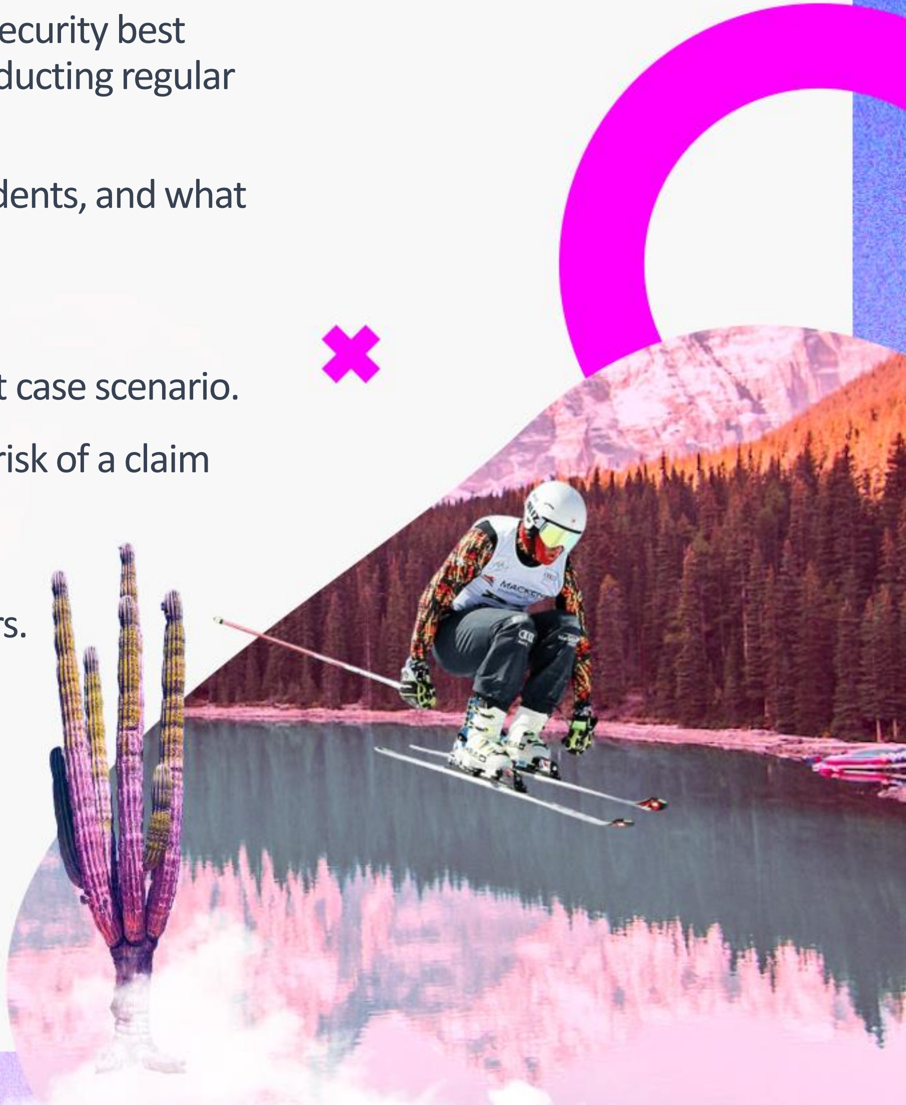
BlueRock

- **Assess your risk:** Before purchasing cyber insurance, assess your organisation's risk for cyber incidents. This will help you determine the level of coverage you need and ensure you're not paying for unnecessary benefits.
- **Understand what is covered:** Cyber insurance policies can cover a wide range of incidents. Make sure you understand what is covered by the policy and what is not.
- **Read the exclusions:** Common exclusions include:
  - Bodily injury and property damage
  - Prior known facts or circumstances Intentional or fraudulent acts
  - Damage to computer hardware
  - Upgrading of an application, system or network
  - Failure or outage of power, utilities, satellites or telecommunication services
- **Check the claims excess:** Make sure you understand the time and monetary excesses that will apply to a claim.
- **Consider additional services:** Some cyber insurers offer additional services, such as risk assessments or incident response planning.
- **Review and update your policy regularly:** As your cyber risk changes over time, it is important to regularly review and update your cyber insurance policy to ensure it continues to provide adequate coverage. Cyber policy wordings are subject to a regular iteration process to try and keep pace with a dynamic and rapidly evolving cyber landscape.
- **Intermediary v. direct:** Consider partnering with an insurance broker versus navigating the direct insurance market.

Applying for or renewing cyber insurance

- Implement strong security measures to reduce your risk of a cyber attack and to demonstrate to insurance providers that you're taking steps to mitigate your risk. This includes training employees on security best practices, implementing firewalls and antivirus software, muti factor authentication and conducting regular security audits.
- Provide accurate and detailed information about your cyber security practices, previous incidents, and what was learned from those incidents.
- Ensure you maintain the risk measures disclosed in your proposal form.
- The more information the better. If underwriters lack information they will assume the worst case scenario.
- Comply with your duty of disclosure. By failing to provide accurate information, you run the risk of a claim settlement being reduced, or avoided altogether.
- Start the process well before expiry of your current policy. In the current "hard" insurance market conditions it's taking longer than ever to source terms from insurers and underwriters. Timing may also impact the premium payable.

Completing a cyber insurance proposal can be a complex process, and it may be helpful to work with an experienced cyber security professional or insurance broker to ensure that your businesses risks are properly assessed and coverage needs are met.



Cyber insurance pros and cons to consider

Pros:

- **Financial Protection:** Cyber incidents can be costly to recover from, especially for SME businesses.
- **Liability Coverage:** This can include costs associated with legal fees, settlements, and damages to third parties.
- **Risk Management:** Insurers often provide risk management services and tools to help policyholders mitigate their cyber risks and prevent incidents from happening in the first place.
- **Reassurance for Stakeholders:** A policy can help demonstrate to customers, investors, and partners, that a company takes cybersecurity seriously and has measures in place to mitigate the risk.

Cons:

- **Cost:** Cyber insurance premiums can be expensive, especially for SME's. The cost of coverage may not be justifiable for lower risk activities.
- **Coverage Limitations:** Cyber insurance policies have limitations on the type of incidents covered, limits, and the excess payable.
- **Lack of Standardisation:** The cyber insurance market is still evolving, and there is a lack of standardisation of terminology, coverage, and pricing, making it difficult to compare products.
- **False Sense of Security:** Cyber insurance can provide a false sense of security if businesses rely solely on insurance to protect them from cyber risks. Companies still need to implement strong cybersecurity measures and practices to prevent incidents from happening in the first place.

BlueRock

Is cyber insurance worth the money?

- Cyber insurance provides financial protection and support to businesses in the event of a cyber attack or data breach, the costs of which can be crippling if uninsured.
- Cyber insurance provides liability coverage in case of legal action, as well as provide access to resources such as cybersecurity experts and incident response teams - resources a typical SME may not be aware of, or may not be able to afford to engage otherwise.
- Cyber insurance can demonstrate to customers and partners that a business takes cybersecurity seriously, which can improve trust and reputation.
- While cyber insurance comes at a price, the cost of the policy is rarely discussed when a claim occurs.

Overall, cyber insurance can provide peace of mind and help businesses mitigate the financial and reputational risks associated with cyber threats.