DP Computing
Simplifying Your IT

Tackling Your Insurers' IT Requirements

Have you recently renewed your business insurance or received questions from your provider about how you protect your IT infrastructure and data? If so, you are certainly not alone.

Insurance companies are increasingly asking businesses about their cybersecurity when reviewing policies. They are handing out long questionnaires that include detailed questions that impact your coverage and premium costs.

We know this situation can be stressful if you are not techno-savvy or lack dedicated IT support. But do not worry, by working together, we can make sure you are taking the proper steps to protect your business while also satisfying your insurer's needs.

DP COMPUTING

THE INCREASING RISKS TO BUSINESSES FROM CYBERTHREATS

All sorts of businesses – from bakeries to contractors to boutiques – rely on computers to run their operations. That means they have customers' details, pricing lists, supplier contacts all stored in a digit format. One slip-up, and bam the bad guys have that information and hold it for ransom, release it to the world or much worse!

It makes sense that insurers want to protect their bottom line and acknowledge the increasing cybersecurity risks to the businesses they insure.

For example, during a ransomware attack, a company may need to:

- call in investigators to determine what has happened and the extent of the damage;
- recover the data and rebuild systems;
- send breach notifications to clients, patients, regulators, or customers;
- consult with PR firms to repair their reputation.

The costs associated with all these items can be costly for both the client and the insurer.

Thus your insurer will want to know what cybersecurity you have in place to determine how much of a risk you are.

WHAT KIND OF QUESTIONS WILL THEY ASK?

Insurance providers will generally want to know:

- Do you store sensitive customer or financial information digitally?
- If so, how do you back it up to protect against data loss?
- Who is responsible for day-to-day management of your IT systems?
- How do you secure important email communications?
- What security measures do you use. These can include such things as:
    - Strong password policies.
    - Multi-factor login authentication (MFA, 2FA).
    - Security software in use (EDR, MDR, XDR etc).
    - Firewalls.
    - Email filtering.
    - Website site filtering.
    - Regularly update your operating systems and software.
    - What employees have access to what information.
- Whether your employees receive cybersecurity training?

The level of scrutiny also scales with industry-specific regulation and compliance. Healthcare, finance and others already face strict security standards.

PRIORITISE CYBERSAFETY, NOT JUST PREMIUM SAVINGS

While some businesses have robust cybersecurity practices and dedicated IT staff to thoroughly answer these questions, many small companies are still learning the basics of digital safety. Don't feel ashamed if you're in the latter group as all of us had to start somewhere.

This type of assessment exposes how much ground remains for most small operations. Even simple things such as enforcing password policies and keeping software updated are often overlooked in daily operations. Thankfully, affordable solutions exist for businesses at any stage.

Far too many view compliance solely as a box-checking expense to reduce insurance costs. But as threats increase, cybersecurity is truly a long-term investment in more than just policy premiums; it relates directly to the health of your business overall. Downtime from an attack can cripple cash flow and destroy customers trust in your business. Prevention offers both financial protection and peace of mind.

Our goal is to guide businesses of any size or sector through building secure, sustainable practices. Rather than fear compliance issues, view this process as an opportunity to help further secure your business.

WE'VE GOT YOUR BACK

As IT experts, let us guide a full review of your security posture based on your insurer requirements. We can address any gaps with targeted, affordable solutions that are tailored to your unique needs and budget constraints.

Feel empowered to answer your insurer's questions thoughtfully and remain covered without exposing yourself to undue risk.

Doesn't that sound like a load off your mind?

Get in touch, and let's make a plan to tackle this proactively together as a team.

DP COMPUTING

08 8326 4364

(Adelaide – Head Office)

02 7902 5169

(Sydney)

support@dpcomputing.com.au

https://www.dpcomputing.com.au/

facebook.com/dpcomputing