medic mall

the smart marketplace

PROTECT YOUR HEALTHCARE BUSINESS FROM

CYBER THREATS

Follow our steps to help protect your medical business from CYBER THREATS. A Single cyber-attack could seriously damage your healthcare business and its reputation.

Protect your business from cyber threats

- Back up your data on a regular basis
- Secure your devices and network
- Encrypt sensitive operational and patient data
- Ensure you use multi-factor authentication for all logins
- Monitor the use of computer equipment and systems
- Put policies in place and train your staff to be safe online

It's simple, it's secure, and it's free to join!
Sign up NOW! Click our QR code below:

Sign Up & Login to MedicMall, to learn more from our trusted supplier partners below:

Cyber Security IT Services:

Cyber Insurance Services:

Cyber Advisory Services:

CYBER SECURITY IT SERVICES

The Security Threat We Can Help Eliminate

- Being held randsom for your data
- Trojan affecting the network
- Keep your practice data safe
- No patient data loss
- No practice down time
- Strong backup in the event your are affected

Why Are Practices Targeted by Hackers?

- They look for high-income earning businesses
- They look for practices that don't have security in place
- Perceived lack of knowledge in IT by practice staff
- Medical Data Sensitivity
- Valuable information easy to ransom

What Are Some Available Solutions?

- Firewalls for Medical Services
- Software Firewalls
- Anti Virus Software
- Anti Malware Software
- Email Security
- 24/7 Anti Virus Monitoring

CYBER INSURANCE SERVICES

A quality policy should address each liability or circumstance

Personal Data Liability
A breach concerning personal information and data protection

Corporate Data Liability
Breach of corporate information

Outsourcing
Breach of data protection by an outsourced provider where the policyholder is legally liable

Data Security

Damage resulting from any breach of duty that ends in:

- malicious contamination
- denial of access attacks
- theft of an access code to a computer system
- destruction/corruption, modification, damage or deletion of data
- physical theft of hardware

Data Disclosure
Due to a breach of data security

Defence Costs
In respect of any litigation brought by a data protection authority

Cyber Extortion
Extortion loss incurred as a result of a security threat

Data Administrative Investigations
Costs and expenses for legal advice and representation in connection with a formal investigation by data protection or other authority

Fines
Insurable fines and penalties imposed by a government authority, data protection or regulatory authority for a breach of data protection laws or regulations

Notification and Monitoring Costs
costs and expenses of the insured if legally required and/or voluntary disclosure to data subjects if required

Reputational Repair of the Company and Individual
Reimbursement of costs incurred in relation to reputational damage due to a claim covered by this policy

Media Content
That results in an infringement; plagiarism, piracy or misappropriation or theft of ideas; libel or slander committed without malice; or an intrusion, invasion

Network Interruption Insurance
Loss of Net income (net profit or loss before income taxes) that would have been earned; if not for a security failure/breach.

Why use a Risk Advisor

Over the last 30+ years, we have continuously proven to our clients the value we bring as their specialist insurance broker and risk advisor. Many Doctors have benefited from our services which include:

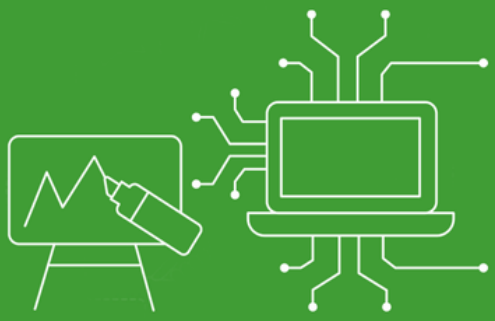
- **A qualified representative** to help you understand and navigate pitfalls such as coverage limitations, the duty of disclosure, retroactive cover, breaks in practising medicine, contractual arrangements between doctors and what it means to you.
- **Claims** – experienced claims handlers to back you up when you need it most.
- Access to **multiple insurers and policy comparisons.**
- **A qualified representative** to help facilitate group covers and discounts
- A qualified representative to call upon whenever you need help, someone that works for you.

CYBER ADVISORY SERVICES

With guidance from our Cyber Security and Privacy risk consultants, you can drive your healthcare business forward with confidence, knowing your most important assets are protected.

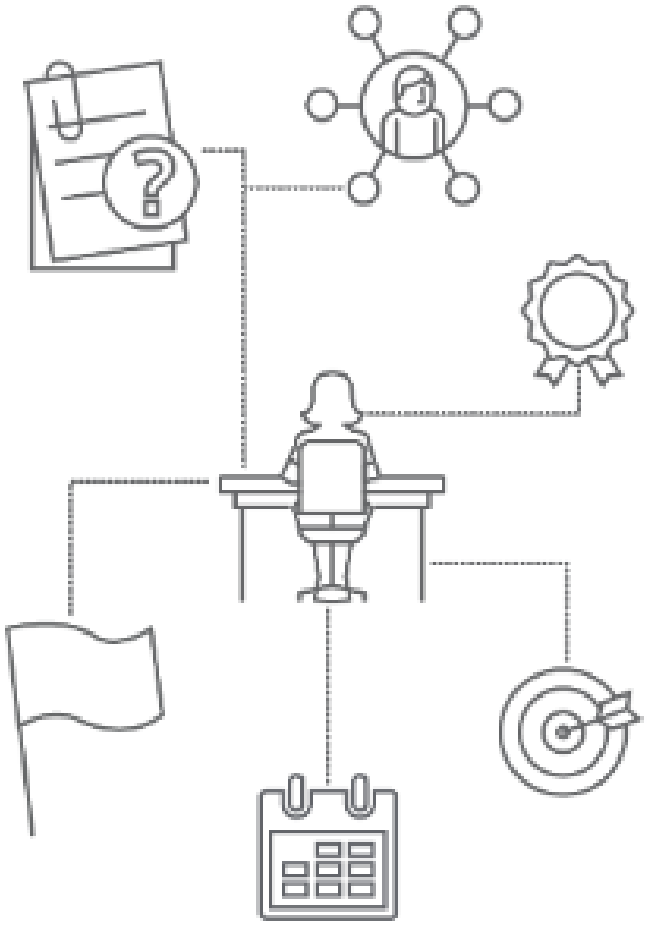
We work with you to identify your organisation's highest strategic risks and, after comprehensive assessments using proven techniques, we help you design or strengthen your system controls, and adapt your policies and procedures surrounding security architecture, access, monitoring procedures and more.

INFORMATION & CYBER
SECURITY RISK



Therefore, healthcare businesses need to employ enterprise cyber security and cyber resilience to ensure their most important assets are protected. As cyber security continues to affect the bottom line, the need to continually assess cyber risk and improve your security program is paramount.

We focuses on the controls to prepare/identify, protect, detect, respond, and recover in an information technology environment, to drive enhancements to the availability, integrity, or confidentiality of IT systems and associated information and services.



IF YOU HAVE ANY QUESTIONS, PLEASE CONTACT US

MEDICMALL CONTACT

1300 950 555

www.medicmall.com.au

info@medicmall.com.au

Suite 5a, Level 1, 28 Burwood Road
Burwood NSW 2134