# Cyber Security for Health Practices and Businesses

*Effectiveness can be affordable*

**The health industry is under attack. The Australian Cyber Security Centre says that the cost of remediation for EACH incident – for a small practice or business of less than 20 employees – is $40,000. For a medium business, 20 to 199 employees – it's more than double that. And this does not count the cost of the impact on the practice, its reputation and its ongoing viability. *Cyber security is no longer a discretionary expenditure.***

## Are your cyber defences healthy?

Too often, protection of technology systems has been treated as an add-on, and, sadly, often a discretionary add-on. "We're too small." "No-one would be interested in us". These responses unfortunately reflect the state of the cyber protection that has been rolled out by practices and businesses across the health sector.

Who is responsible for this aspect of your business? Does that person really know the risks and do they understand just what level of protection is delivered by the protocols and systems that might be in place, if there are any?

## "The Privacy Act doesn't apply to me" – Guess again!

Regardless of turnover, the Privacy Act covers any business that is:

- A health service provider
- Trading in personal information
- A contractor that provides services under a Commonwealth contract
- An operator of a residential tenancy database

The Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 increases the maximum penalties for serious or repeated privacy breaches from the current $2.22 million penalty to whichever is the greater of:

- $50 million;
- Three times the value of any benefit obtained through the misuse of information; or
- 30 per cent of a company's adjusted turnover in the relevant period.

## Why cybersecurity is often left in the "too hard" basket?

Although cybersecurity is vital in healthcare, and the risk of losses and penalties very high, all too often small health providers struggle to get it implemented due to:

- Lack of IT security skills in the business
- Perceived high cost of implementation and maintenance
- Underestimating the risk to their data, continuity of operations and reputation

## A complete approach to cyber security

Ideally, your cyber protocols would cover the following:

- A regular review to identify potential critical risks and issues.
- Having a cyber-aware and educated employee, using up to date and renewed training resources.
- Security technology that provides
  - An effective firewall
  - Web Security
  - Secure remote access
  - Email Security

## Protect your patients, professionals AND suppliers

Protecting patient data is paramount. So is ensuring continuity of service for your clients, professionals and suppliers. A malware breach would not only compromise your data and reputation, but also bring down the entire business. Can you afford to be offline for hours or even days? What would be the cost of losing your data – perhaps forever? Putting in place the right systems means you can rest easy knowing that the risks have been reduced, as well as provide proof of your secure environment.

With the flow of any number of employees and professionals in your practice – casual workers, locums, VMOs, consultants, allied health professionals – threats can enter your network through one of them inadvertently accessing a compromised website or clicking on a malicious link sent through email. Even with the best intentions, it's all too easy for cybercriminals to enter your systems and compromise your data.

HEALTH SERVICES
by RSM

## RSM's Risk Advisory offering for the health sector

Our Health Services Cyber Security Package is a simple, quick and cost- effective approach to understanding and managing key cyber security risks within health practices and businesses. When designing the package, the focus was placed on covering the keys areas of cyber risk: people, process and technology. As a result, the package we have created covers a high- level security review, setting up of a user-based policy and associated training, and technology tools to help mitigate ransomware threats.

MENLO SECURITY

RSM

## What we deliver

The Health Services Cyber Security Package includes the following key components:

- **Cyber Security Review** – a cost effective self- service audit of cyber security risks and maturity for your practice or business
- **Security policy and a user education module** – aimed at providing the guidance and training necessary for employees to be cyber-aware and safe
- **Security technology** – covering the following:
  - Firewall
  - Web Security
  - Secure Remote Access
  - Email Security

## How the Health Services Cyber Security Package can protect your business

The Health Services Cyber Security Package is tailored to help health practices and business take effective but affordable steps to protect people, process and technology.

- The initial review puts a line under the starting point of improved protection.
- The user education module ensures that current AND new employees, contractors and locums have access to the right resources before they can cause damage.
- The security technology puts up your defences and keeps them current and operating around the clock.

## Sample Package Costing

Using the information below, a health practice of 20 employees can implement this protection package for one-off costs of $570 per employee and ongoing costs of $600 per employee per annum.

## The Health Services Cyber Security Package:

### Scope

- A self-service security assessment designed to provide SMBs an idea of their current security gaps. The offering includes 8 hours of a consultant's time to assist with the completion of the assessment.
- A customisable user-based security policy and a user education module. This service includes 8 hours of a consultant's time to assist with the customisation of the security policy and running one train the trainer sessions for the user education module
- Provision of security technology delivered on premises and via the cloud as a fully managed service including the following:
  - Cloud Firewall
  - Web Security
  - Secure Remote Access
  - Email Security

### Pricing

1. Self-service security assessment – $5,900 for up 25 users; $7,900 for up to 50 users; $11,900 for up to 100 users (once off)
2. User based security policy and a user education module – $4,500 (once off)
3. Security technology – $50 per user per month, assuming a 3-year agreement

Prices do not include GST and are based on full payment in advance annually.

### Support

Please note that the implementation and support for the security technology will be provided by Menlo Security. Please review their End User Licensing Agreement and Support Agreement prior to signing.

### Assumptions and Exclusions

1. Client will provide access and support needed to make any endpoint and network changes necessary to deploy the service
2. The service does not include an Incident Response Plan or incident response if there is a security issue
3. This service does not include any remediation services required revealed by the self-service security assessment
4. The policy document provided is a user focused security policy. Broader, organisational wide and IT specific security policies are not included. IT Disaster Recovery Plan and BCP are excluded
5. The security assessment is not a penetration test or other deeper technical assessments.

Services related to 2 to 5 above can be provided at an additional charge.

**For more information on how to protect your health practice or business, please contact our Risk Advisory cyber specialists:**


**Ashwin Pal**
Partner, Sydney
**T** 02 8226 4500 **E** ashwin.pal@rsm.com.au

**Darren Booth**
Partner, Melbourne
**T** 03 9286 8158 **E** darren.booth@rsm.com.au

**Riaan Bronkhorst**
Principal, Perth
**T** 08 92619272 **E** riaan.bronkhorst@rsm.com.au


**Or contact your local RSM adviser for an introduction to our specialist team.**



MENLO SECURITY

RSM