Is cyber insurance worth it (and what is it anyway?)

Chris Mariani is the Director at Medical and General Risk Solutions.

Chris Mariani explains the importance of cyber insurance.

22 February 2019 marked the first-year anniversary of the Notifiable Data Breach (NDB) Scheme under the *Privacy Act 1988*. The NDB Scheme requires entities which are subject to the Privacy Act to notify the Office of the Australian Information Commissioner (OAIC) and all impacted individuals of an "eligible data breach". For a breach to be classified as an eligible data breach – all three criteria as follows need to apply:

1. *there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds*
2. *this is likely to result in serious harm to one or more individuals, and*
3. *the entity has not been able to prevent the likely risk of serious harm with remedial action*

In the period 22 Feb 2018 to 31 December 2019 Health businesses notified 163 breaches under the NDB Scheme, more than any other industry. **Refer to the reports by clicking here.**

Every week we work with clients who have privacy breaches ranging from a fax going to the wrong address, or personal or health information being accidently sent to the wrong patient or hospital. The reality is there are far more 'human error' privacy breaches, than the cyber criminals successfully breaching a practice's IT security. The only way to guarantee you will not have a privacy breach, is to simply not collect any personal information in the first place!

There are a number of potential reasons why healthcare 'tops the tables' under the NDB Scheme:

1. Most organisations are not subject to the Privacy Act (or NBD scheme), until their annual revenue reaches $3 million - whereas healthcare organisations are subject to the Privacy Act from $1
2. Loss of, or access to healthcare information is generally regarded as likely to result in serious harm, which is one of the triggers of the requirements to report a data breach under the NDB scheme.
3. Doctors have ethical duties and are likely more aware of their obligations to report matters, and cyber criminals see healthcare organisations as attractive targets due to the sensitive information they hold, the value of the data on the dark web and the willingness of the practices to pay the ransom to recover their data.

The OAIC website notes:

Health information is regarded as one of the most sensitive types of personal information. For this reason, the Privacy Act 1988 (Privacy Act) provides extra protections around its handling. For example, an organisation generally needs an individual's consent before they can collect their health information. In addition, all organisations that provide a health service and hold health information (other than in an employee record) are covered by the Privacy Act, whether or not they are a small business.

After a significant privacy breach or cyber event hits the media, I often receive calls from medical practices enquiring about cyber/privacy insurance, and what, if any cover, exists within their existing medical indemnity or other insurances. Usually the discussion goes along the lines of:

Hi Chris, I think we need a cyber/privacy breach policy. How much does it cost?

Hi Dr, can we first talk about your 'privacy framework' and whether you are confident you are compliant with the Privacy Act. This is your first layer of defence and in my view you need to first get compliant, and then consider the value of cyber/privacy insurance, which can range from less than $1,000 to maybe $5,000 as a small/medium practice, but this does depend on your practice size, what policy limit and covers you purchase and the quality of your IT security and privacy processes. While the insurance can pay for the costs associated with a cyber or privacy event, it won't necessarily protect your reputation, if you're dragged through the papers in a fashion where it shows you failed to take even the most basic precautions to protect patient privacy. Not only that, but you largely remove the risk of a privacy fine of up to ~$2million where you can demonstrate you have taken reasonable steps.

Thanks Chris, what's a privacy framework? I'm not really sure what we are required to do under the Privacy Act. I think we have a privacy policy somewhere, what else is needed? I think our IT security is pretty good, we use X IT.

Essentially Dr, the Privacy Act requires you to take 'reasonable steps to protect patient privacy'. You are dealing with what is regarded as 'sensitive information' so there is a higher expectation on you. To say you are compliant, you would need to be able to demonstrate:

- *You have a Privacy Policy that complies with the Australian Privacy Principles and other relevant documents such as a Breach Response Plan, Patient Consent forms and other documents.*
- *You have trained your staff, both at induction and ongoing – so for example running an annual staff session on privacy.*
- *You have done an assessment of your IT providers, security, backups, and have considered options to collect, store and use personal information. You also make sure they comply with the Privacy Act and there's a strong contract in place where they are there to assist you meet your privacy obligations, such as notifying you and assisting with a 'Notifiable Data Breach'.*
- *Plus there's lots more. There is an excellent resource on the OAIC website.* ***Refer to OAIC framework here.*** *This talks about a 4 step framework, starting with embedding a culture of privacy that enables compliance. Please go and have a read and see how many of the items on the checklist you are confident you can tick off.*

That sounds like lots of work Chris. I'm not confident we are compliant.

That's the usual response I get Dr, now is a good time to start. Put privacy compliance at the top of your practice managers to-do list. They should be your 'Privacy Officer' which is another requirement in the framework. We have a 'Privacy Starter Pack' available to clients and can also come and help you set up your framework. Usually in 2 days, we can help your PM draft your key documents, run staff training, help you ask your IT guys the right questions (like a mini-audit) and put you on the road to having a framework which your PM can then own and run. I suggest start a conversation with your IT guys now. I'll send you a list of draft questions. Ask them to give you a written 'bullet point' response to each question. I'll also send you some info on what the cyber/privacy insurance covers and we can have a discussion on that once you have digested the info.

EXAMPLE QUESTIONS TO SEND TO YOUR IT CONSULTANTS:

Note: The following questions are draft questions for you to send to your IT consultants. Change/add/delete as applicable to your situation. You are essentially asking for their assistance to do a 'mini-audit' and to help you demonstrate you are taking reasonable steps (and if not, then what you may need to do to improve your IT systems).

- Can you explain our current IT structure and provide some options, should we be server in rooms, cloud based, or a hybrid structure. What are the benefits and risks of each, as well as cost considerations?
- Do you believe we are taking reasonable steps to protect patient privacy, secure and back-up our sensitive data (from patient records and personal information, to company financials)?
- Where do we rate according to other practices you manage?
- What else should/could we do to further improve our IT security?
- Please provide us an overview of all of the security features and steps currently taken to protect our data, including firewalls, virus protection, multi-site backup and other security features.

- In the event of a cyber-attack on our system (eg staff member opens the cryptolocker virus), would hackers gain entry or be able to lock our system down preventing us from running our business? If they are successful, how long would it take to restore our system and be back up and running?
- Can we have a copy of your breach response plan, disaster recovery plan and other documentation which shows what you do in the event of a breach?
- Please confirm you are compliant with Australian Privacy Laws. Please send me your current Privacy Policy. Can you also send me the latest contract we signed with you?
- What training can you provide to staff which would assist (we understand people are often the weak point so what can we do to lessen our risks)?
- Does any of our data leave Australia (eg backed-up on an overseas server)?

CYBER/PRIVACY INFORMATION AND ROUGH PRICING

It is important to understand:

1. there are many different risks that can arise from a privacy breach or cyber event. I use both these terms as losing a hard-copy medical record, or sending patient test results to the wrong fax number are examples of privacy breaches. A cyber event could involve an event where no 'personal information' is lost or accessed, but where sensitive company information may be.
2. there will likely be some insurance cover under a doctor's/practice's medical indemnity cover. Each of the medical indemnity insurers differ in what they will cover (with some being far superior to others). Generally, under a doctor medical indemnity - insurers consider a patient bringing a 'civil claim' (e.g. a legal demand for $1million) for a breach of privacy as covered – as the privacy breach is of a similar nature to allegations of medical negligence – such as failure to follow up inconclusive test results which leads to delayed or missed diagnosis). Most insurances have been broadening out their policies to pick up some of the additional risks, such as a small limit for the potential privacy fine and/or the costs to deal with a privacy breach under the NDB scheme. BUT, the cover under medical indemnity does not cover every risk that is covered under a cyber/privacy policy. So asking your medical indemnity insurer "am I covered for a privacy breach" Should be will likely not be a simple Yes and No answer.

So what does a cyber/privacy cover?

There are a number of specialist insurers who each offer differing levels of cyber/privacy cover. Generally these policies are purchased through insurance brokers and advisers as many of these specialist insurers will not deal with the public direct.

Cyber cover is in many ways like medical indemnity. While you are buying an insurance policy, what you really get is access to a range of experts who can help you through the initial event, provide advice, arrange for experts such as lawyers, IT security/forensics specialists, PR consultants to help you deal with media issues. Secondly, these experts are funded by the insurer, along with other costs you may be required to pay, such as the privacy fine, credit monitoring (if say patient credit card details were stolen) and other costs. Thirdly, policies can also pay the ransom payment and your lost revenue following the event.

In some policies, cover also extends to Social Engineering, Phishing and Cyber Fraud (e.g. a supplier is hacked and the hackers access their system and see they regularly send you an invoice for $10,000. The hacker simply alters a PDF invoice they have access to, updating it with new payment details linked to their bank-account. Your practice manager receives what looks to be a genuine email and invoice and pays the invoice without question. Several weeks later the fraud is discovered when the real supplier calls and asks why their invoice hasn't been paid). TIP: While this insurance is available the policy requires you to take steps to verify payments, so without appropriate financial controls, the insurance may be worthless. This cover for loss of your money through social engineering is often offered as part of a Management Liability policy under the 'crime section' (each insurer does this differently so important you seek advice on what suits you circumstances).

So, in short, what does a cyber/privacy cover:

Cover	Summary
Your costs to deal with a cyber breach	Lawyers, IT experts, forensic investigations, notifying patients, PR consultants and other experts.
Cyber Business Interruption	Pays your lost revenue (usually no cover for the first day).
Systems Damage	Pays costs to restore data, programs and networks after a hacking/malicious event.
Cyber Extortion	Ransom amounts paid and associated costs
Third Party liability	Privacy fines, civil claims and liabilities you may be required to pay.
Social Engineering, Phishing and Cyber Fraud	Loss of your money through cyber fraud. Note some insurers don't cover this in the cyber policy and include it within a Management Liability.

Not only do policies differ in cover, so does the insurers expectation of what IT security and privacy compliance you are required to abide by. For example, insurers would expect all systems, computers, storage devices are password protected at a minimum. Further, I would not want to lodge a claim with an insurer where the Privacy Fine is $2m as the practice clearly was not even close to Privacy Compliant (potentially you give an insurer a reason to attempt to deny a claim under your 'Duty of Disclosure' to disclose facts which may be relevant to the risk).

So what does a cyber/privacy cost

Providing an exact cost is difficult as insurers rate the policy off various factors including revenue, staff numbers, policy limits and covers selected, as well as the quality of your IT security and other factors. As a guide for small medical practice of say $1m annual revenue, a policy with a $1m policy limit will likely cost ~$2,000 and a $3m revenue practice may be closer to $3,000.

Want to know more?

If you would like more information in relation to this article, please **contact us** for an introduction to **Chris Mariani**.