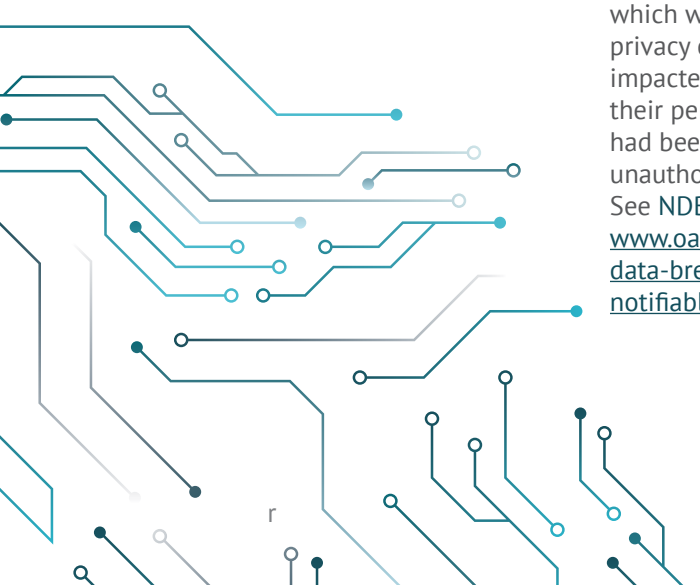
Learnings from a cyber insurance claim

Negotiating an insurance claim with insurers has many of the same characteristics as poker – generally the person that knows the most, is the expert, knows the rules of the game and that has the deepest pockets, tends to win. Even when holding the right cards, the inexperienced player can be talked out of winning. When lodging an insurance claim, the parallels are many:

- you've got to be holding the right insurance policy to start with;
- you've got to know how to play the game, how to ensure the insurer pays out - according to the technical and legal words in the insurance contract; and
- you've got to know how to prepare the information so the insurer will pay the claim, such as how to prepare financials to prove your lost revenue.

Recently I helped a GP clinic finalise a cyber hacking event, covered by a cyber-insurance policy they held. The practice owner opened a phishing email and clicked… and by doing so, their entire system was encrypted with Ryuk – a type of ransomware that uses encryption to block access to a system, device, or file until a ransom is paid. Ryuk demands payment via Bitcoin. In our case the demand was for 15 Bitcoin (so circa $150,000).



The practice immediately contacted their IT consultant. A decision was made to not pay the ransom and instead to wipe their systems and re-boot from a backup. All of the local backups on their server were compromised, so they used the overnight cloud backup. This process took several days (with the majority of services up and running within 24 hours), but the impacts lasted for weeks, key issues were:

1. All of the electronic medical records for patients that day (the event occurred early afternoon) were lost. This meant all those patients had to be recalled and a new record of the consult entered.
2. Limited or no access to IT for approx three working days while the systems were rebuilt. Lost revenue, impact to patient continuity of care. The IT bill at this stage has hit almost $30,000 as the IT team were working around the clock to get the practice back fully operational.
3. There was some data that simply could not be recovered such as some pathology results. This resulted in another ~$40,000 of costs to get the data manually back into the medical records system.
4. A breach assessment had to be conducted to see if the matter was a Notifiable Data Breach, which would then mandate the privacy commissioner and every impacted individual to be notified their personal/health information had been "lost or subjected to unauthorised access or disclosure". See NDB Scheme: www.oaic.gov.au/privacy/notifiable-data-breaches/about-the-notifiable-data-breaches-scheme/
5. As the practice used the My Health Records system, another breach assessment on whether the security or integrity of the My Health Record system was compromised, and if so, then notification to the Australian Digital Health Agency Healthcare. You can read more about this at My Health Record: www.myhealthrecord.gov.au/for-healthcare-professionals/howtos/manage-data-breach
6. Lots of time and stress placed on the practice owners and managers to ensure during the coming weeks and months. While the practice returned to normal operations within a few days these matters drag on with post action items, insurance claims etc.

At the initial stage of breach investigation, it became apparent the IT systems had only been encrypted and the hackers had not accessed any of the personal information (or any data whatsoever). The IT consultants did an excellent job documenting why no data had left the practice servers – this meant the lawyers appointed to assist in the breach assessment were able to advise quickly their initial view:

> *All patients listed in the appointment book… were recalled and important medical information restored, I do not think that any notification needs to be made to My Health Records. I also do not think that any notification needs to be made to the Office of the Australian Information Commissioner (that is, I do not think that there has been an eligible data breach). I congratulate you and your practice on the swift risk management actions you took in recalling the patients and restoring the data.*

This initial assessment was later formalised confirming all systems were restored, all data re-entered and no unauthorised access.

INSURANCE ISSUES

Despite my advice to them the year before, the client hadn't purchased a specialist cyber/privacy insurance policy. Luckily however, as a part of the medical indemnity they had purchased, they were provided with a 'free' cyber policy. The client lodged a claim under this policy and dealt direct with the insurer.

The insurers involved did two things initially:

1. **Breach assessment** – sent the client numerous links, information and essentially said to the practice "make your own decision on whether you believe this is a Notifiable Data Breach". The client felt lost and helpless.
2. **IT costs** – advised the client as they felt the IT consultant was negligent in not having a better backup, they would only pay approx $3,000 of the ~$30,000 invoice (after deducting the excess)

The client contacted MGR asking if we could take over management of the claim. Since that time:

1. The insurer appointed and paid for lawyers to undertake the breach assessment, which as noted previously, provided legal advice the incident was not a Notifiable Data Breach and didn't compromise the My Health Record system.
2. The insurer fully paid:
    a) the ~$30,000 IT fees less the excess,
    b) the extra data recovery covers of ~$40,000,
    c) the lost revenue for the three days of impacted trading (time excess of one day)
    d) the employee overtime incurred due to the cyber event

The total paid by the cyber insurer was ~$90,000.

So while the client was fortunate to end up with insurance to cover all of the costs and provide them the legal advice and guidance, they didn't know how to ensure their claim was paid and the insurer deliver on their promise to assist, in accordance with the terms of the policy. As I often say to clients,

> *I can buy a scalpel, doesn't mean I can do my own surgery... You can buy an insurance policy direct from an insurer, doesn't mean it's the right one, or that you'll know how to use it when you need to claim.*

On finalising the claim, I asked the client a few questions on what they learnt. Here's a summary of their commentary (some info redacted to protect privacy):

- **What did you learn following this cyber event?**

  I have learnt a lot including putting data breach response plan in place and understanding better the Notifiable Data Breach Scheme which determines if the breach is to be reported to OAIC and the patients

- **What have you learnt about IT security?**

  Maintain good computer habits, limit network access, use of antivirus and firewalls and how to better use password and passphrases.

- **What extra IT security or other steps have you put in place to prevent the same thing happening again?**

  A lot of changes have been put in place by my IT, we are also going to do cyber security training. IT security and privacy are now on the agenda!

- **How important is it to have an IT provider who will drop everything and come straight away and fix the system, data etc.**

  My IT is a guru and committed to his work. He got my business back t o function within 24-48 hours. He didn't sleep for probably five days. It is rare to find someone who would drop everything and get your business back up in 24 hours. The forensic team commended him for his great work.

- **Anything else you want to write about/ was MGR helpful?**

  You cannot ask for a better insurance broker than Chris Mariani. The support I received during the cyber-attack was incredible. I appreciate his untiring communication, numerous meeting, back and forth between us and the insurer. He got them to pay, when we had no idea how to.

If you want to read a little more about privacy compliance and cyber insurance, read my article at https://mgrs.com.au/cyber-insurance/ – this has some draft questions you should be asking your IT consultants about IT security, backup etc. I am also constantly banging on to clients about the need to develop a privacy framework, a part of this requires the practice to assess their IT security, staff training, backup and recovery processes and other risk management measures. You can read about privacy frameworks at the shortcut to the OAIC website: **https://bit.ly/3jto7UP**

CHRIS MARIANI
P: 0419 017 011
E: chris@mgrs.com.au

MGR
MEDICAL AND GENERAL RISK SOLUTIONS