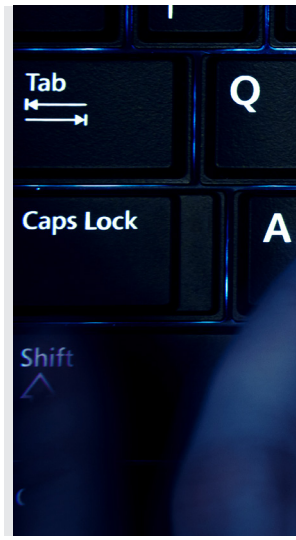
Risk managing the Privacy Amendment Bill 2016



JAMES WARWICK
Senior Account Executive, Medical & General Risk Solutions

P: 1300 883 059

E: james@mgrs.com.au

MGR
MEDICAL AND GENERAL RISK SOLUTIONS

Privacy breaches affect hundreds of millions of electronic and paper based records a year. The cost of cyber crime globally is even more sobering with losses attributed to it expected to rise from the estimated $450 billion calculated in 2016[1] to a truly incredible $1 trillion in 2021 (with some estimates putting the upper limit at $6 trillion[2]).

It becomes even worse when one considers a recent study conducted by the Information Systems Audit and Control Association (ISACA) which determined that only 38 per cent of those organisations surveyed believed they were prepared to meet the rising threat of sophisticated cyber-crime[3].

Given the financial cost and lack of industry preparedness, the government has passed new legislative requirements for the handling, storage and dissemination of sensitive client information. This legislation also includes mandatory reporting should unauthorised parties compromise a client's confidential information.

The legislation is targeted primarily towards organisations with an annual turnover of more than $3 million, however the Privacy Act also applies to specific businesses with an annual turnover of under $3 million- principally private sector health services providers who are subject from the first dollar earned.

Under the new legislation, if you have reasonable grounds to suspect that an eligible data breach has occurred, you will be obliged to investigate and assess that breach and notify your findings to the Australian Privacy and Information Commissioner.

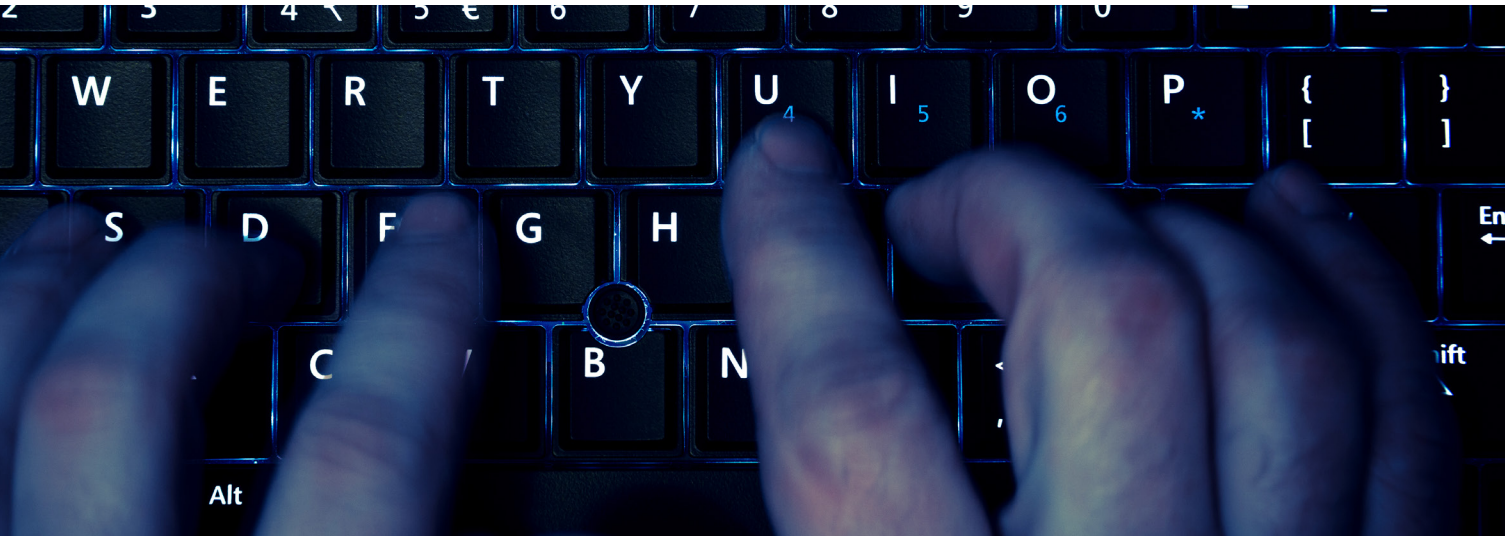
Your notification to the commissioner will require you to:

- prepare a statement setting out your businesses identity and your current contact details;
- provide a description of the breach, including details on the type of sensitive information that has been compromised;
- provide recommendations about what individuals should do in response to the breach;
- notify the contents of the statement to each of the affected individuals to which the relevant information relates or are at risk from the breach; and
- if not practicable to notify affected individuals, publish a copy of the statement on your website (if any) and take reasonable steps to publicise the contents of the statement.

If you've been lax with your privacy security policies - and let's be honest there would be very few of us that could say that our IT procedures in particular are impeccable - this legislation is a good wakeup call that the government is now taking data security and privacy breaches very seriously and, as a consequence, so should you.

References

1. Hiscox Cyber Readiness Report 2017 https://www.hiscox.co.uk/cyber-readiness-report/
2. Cyber Security Ventures 2016 Cybercrime Report http://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
3. ISACA 2015 Global Cybersecurity Status Report https://www.isaca.org/pages/cybersecurity-global-status-report.aspx
4. Verizon 2016 Data Breach Investigations Report http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/



With penalties for non-compliance of up to $360,000 for individuals and $1.8 million for corporate entities and not to mention the associated crippling reputational costs following a reportable breach now is the perfect time to take a good hard look at how you're protecting your client's data and whether or not your existing cyber-security and privacy practices are adequate.

So what can you do to help both meet the requirements as set out under the legislation and at the same time reduce the risk of a Breach? We recommend a one-two combination of proactive and reactive strategies.

Proactive risk management is where you strive to identify and introduce preventative measures to help combat risks before an incident occurs whereas a reactive risk management program should be considered after an incident is identified or confirmed.

Pro-active cyber risk management involves personally introducing steps that can actively help diminish the chances of a privacy breach occurring. Some of the proactive steps you can introduce include:

- Taking the time to understand your obligations under the Privacy Act and get advice where necessary from the relevant experts and ensure your documentation is up to scratch (e.g. new patient consent forms, privacy policy that can be presented to your clients).
- Have contingency plans and procedures set in place in the event of a privacy breach. This involves raising awareness and continuing to educate staff annually about your organisation's internal procedures and how to respond to an actual or suspected privacy breach.
- Ensure your electronic systems are always patched to the latest versions. Most attacks exploit known vulnerabilities that have never been corrected. In fact, the top 10 known vulnerabilities accounted for 85 per cent of successful exploits[4].
- Limit remote access to your systems directly from the Internet to only those individuals, systems and services that really require it.
- If you outsource any of your IT or have arrangement with third parties who will hold or have access to sensitive information, ensure you have contractual provisions in place to ensure they maintain and enforce compliance with the new legislation.

So now, you've implemented a comprehensive proactive risk mitigation program for your office and you're confident you are compliant with the new legislation- excellent!

So what happens if (despite all your efforts to prevent it) you suffer an attack and your client's personal data is compromised? Well this is where your reactive risk management measures come into play and you can fall back on your response triggered safety nets such as- yes wait for it- insurance!

For a set annual premium, a cyber liability policy will allow the insured access to the necessary specialist expertise they will require after an eligible breach (e.g. lawyers, PR and IT specialists amongst others) that normally would be obtained at best at a cost of tens of thousands of dollars and, at worst, given a serious enough breach - millions.

A good cyber protection policy should include at a minimum the following covers:

- business interruption;
- e-theft loss, financial loss due to the fraudulent input of data into a computer system or through a network into a computer system;
- e-threat loss, including the cost of a professional negotiator and ransom payment;
- e-vandalism loss, even when the vandalism is caused by an employee;
- crisis expenses, including the cost of public relations consultants; and
- disclosure liability, including claims by customers arising from system security failures resulting in the dissemination of private information on the internet.