Annelies Moens,
Managing Director,
Privcore

Your core business is data

By Annelies Moens

This article discusses simple and effective steps to mitigate cyber and privacy risks. It is **Part 1** of a two-part series, first published by Legalwise.

As the most-targeted sectors for data breaches reported to the Office of the Australian Information Commissioner (OAIC) in the last year, health service providers, finance, legal, accounting and management services, education and personal service industries that handle personal information need to be aware of key privacy and cyber risks facing their organisations.

The most commonly breached types of data include: contact information, financial details, identity information, health information and tax file numbers. This article focuses on the steps your organisation can take to address your cyber and privacy risks.

The mandatory data breach reporting scheme

The mandatory data breach reporting scheme contained in Part 3C of the *Privacy Act 1988* (Cth) (the Privacy Act) as amended applies to all entities regulated under the Privacy Act. This includes federal government agencies, ACT government agencies, private sector entities with an annual turnover greater than $3 million and some small businesses regardless of turnover, such as health service providers. It also applies to otherwise exempt small businesses, if they handle tax file numbers.

In any event, all organisations should heed the requirements as set out in the Privacy Act, as a data breach can result in loss of customer trust and reputational damage. As outlined further in this article, risks can be minimised through simple mitigation strategies. In a recent survey on 'Consumer views and behaviours on digital platforms' that the ACCC commissioned as part of its Digital Platform Inquiry in late 2018, over 4,300

adults were asked the following: “compared to one year ago, how concerned are you about the privacy of your personal information on digital platforms?” The results showed that 54% were more concerned. Given that customer concerns are escalating, how organisations manage their customers’ data is a matter that requires serious attention.

Top global risks

Two of the top-five global risks likely to eventuate as reported in the World Economic Forum’s *Global Risks Report* in 2019 are data theft or fraud and cyber-attacks. The remaining top risks related to climate change events. In my experience, having worked at the Federal Privacy Commission and consulting globally, common privacy and cyber risks include:

- Over-collection of personal information;
- Never deleting personal information: no data destruction or retention policies in place or acted upon;
- Failure to effectively manage customer expectations, as most information about how personal information is handled is in privacy policies or terms and conditions that are not read or are far removed from data collection points and contexts relevant and/or understandable to the customer;
- Third-party arrangements with vendors and suppliers that may not protect personal information, often due to failure to check supply-chain privacy risks;
- Failure to use multi-factor authentication and encryption; hence insecure email and systems and increased risk of being vulnerable to phishing attacks;
- Human error: for example, emailing personal information to the wrong recipient; and
- Loss or theft of data: for example, losing an unencrypted USB.

> “In any event, all organisations should heed the requirements as set out in the Privacy Act, as a data breach can result in loss of customer trust and reputational damage.”

> "The impact of a data breach can be crippling for an organisation and affected individuals. Cyber incidents often reach the press without the affected entity controlling messaging, which is especially the case if they have been trying to hide the breach."

So, what happens WHEN you have a data breach?

I always like to ask my clients four key questions, and if they can answer these questions, then they are well on their way to being able to manage a data breach when it occurs:

1. How will you know you have been subjected to a data breach?
1. What's the impact of a data breach on your organisation, customers and other stakeholders?
2. How do you minimise the risk/impact of a data breach?
3. How do you implement a data breach response plan?

It is not necessarily immediately obvious when your organisation has been subjected to a data breach. Whilst it only takes hours for data to be stolen or corrupted, once your system has been infiltrated, it can take months and sometimes years for the attack to be discovered. A recent example of this is the Australian National University data breach where systems were compromised in 2018 but the infiltration was only discovered in May 2019. In the 2018 IBM Ponemon *Data Breach Study*, the average time to discover a compromise was 6.5 months. This study included a sample of 24 Australian organisations (representing 5% of the surveyed population). Once the breach is discovered, it can still take months to contain. So, much more

effort and resources are required to detect and contain cyber incidents.

The impact of a data breach can be crippling for an organisation and affected individuals. Cyber incidents often reach the press without the affected entity controlling messaging, which is especially the case if they have been trying to hide the breach. That is a flawed strategy. Reputation and trust diminishes, regulatory intervention may occur, and the breach will have to be reported to the OAIC if it is likely to cause serious harm to affected individuals. Other impacts include litigation, loss of value, such as the decline in share value and loss of business (which was recently experienced by LandMark White due to data breaches) and sometimes businesses can shut down, which is the fate that struck Distribute.IT, a former major web-hosting provider based in Australia.

According to the 2018 Ponemon *Data Breach Study*, the average total cost per data breach in Australia in 2018 was approximately $US2 million. Data breaches caused by third parties, compliance failures or migration to the cloud resulted in higher costs. Costs of data breaches decreased where data breach response teams were deployed or extensive encryption was already in place. Malicious and criminal attacks are the main causes and also the most expensive, at $US108 per record in Australia.

> "It is still important to have a data breach response plan in place, even after taking the above mitigating steps, as in the heat of the crisis, rational thinking will decline, and stress levels will increase.

It is possible, of course, with the right leadership support, to minimise the risk and impact of a data breach. Common mitigation strategies include:

- Only collecting the data needed: be clear about what is optional and what is essential; think about creating lean data rather than big data;
- Have a data destruction plan in place and execute it;
- Have a data breach response plan in place: expect a data breach to happen and practice for it;
- Undertake privacy and phishing training for staff;

- Never use the same password across accounts and use complex passphrases: use a password safe program to create and securely store passwords;
- Enable multi-factor authentication;
- Encrypt all storage devices, including laptops and USBs; and
- Consider cyber insurance and undertake a privacy health check.

It is still important to have a data breach response plan in place, even after taking the above mitigating steps, as in the heat of the crisis, rational thinking will decline, and stress levels will increase. The OAIC has produced guidelines on managing data breaches. The key steps to undertake include:

1. Contain the breach and perform a preliminary assessment within 30 days (or 72 hours if you are also required to comply with the General Data Protection Regulation in Europe).
2. Appoint a lead person to manage the response team. This person can either be an external person, such as a privacy consultant, or an internal person with decision making power.
3. Evaluate the risks associated with the breach.
4. Consider whether the breach is likely to cause serious harm and thus trigger the mandatory data breach reporting provisions. If not, consider voluntary notification in any event as a matter of good practice.
5. Review the incident and take action to prevent future breaches. ●

Part 2, coming in the Conference Edition of the *GRC Professional Magazine,* will include an analysis of the mandatory data breach reporting scheme since commencement on 22 February 2018.

About the Author

Annelies Moens, CIPT, FAICD, CMgr FIML is a widely-recognised global privacy expert and thought leader, trusted by business executives, government and privacy professionals with close to 20 years' experience. She is Managing Director of Privcore and cofounder of the International Association of Privacy Professionals in Australia and New Zealand. Contact Annelies at: operations@privcore.com or visit: www.privcore.com.