IS BURN AND CHURN INEVITABLE UNDER MANDATORY DATA BREACH REPORTING LAWS?

Data Migrators

IBM Silver Business Partner

New laws compelling companies to report data breach events could precipitate increased customer churn for affected business. How should customer retention teams, risk managers and IT work together in this new regulatory environment?

Consumers that exchange personally identifiable information (PII) with a service provider do so based on an inherent trust. Until recently, consumers have had little protection under the law if providers failed that trust but this has changed, bringing serious and immediate implications to bear on companies that collect such data.

In February 2017, the Federal Senate passed the Privacy Amendment (Notifiable Data Breaches) Bill 2016. This put the business community on notice that new mandatory breach reporting laws were to be put in place within a year. Once in effect, these new laws will compel companies to report PII data breaches to the Australian Privacy and Information Commissioner within 30 days. Reporting needs to include the identity of the organisation, a description of the security event, the kind of information concerned, and recommendations to the individual as to how they should respond to the breach.

In this new mandatory reporting environment, there will be little time for the business to deploy counter measures to mitigate the risk velocity of such an event. As news breaks, social media activates. Once affected customers react, those companies that fail in their duty to protect customer data will be rapidly 'named and shamed'.

Along with reputational loss, there are considerable penalties in place for companies and for individuals involved in data breaches. If the Privacy Commissioner determines that a breach was avoidable or if a breached company is a repeat offender, the Federal Court or Federal Circuit Court of Australia can levy penalties of $360,000 for individuals and $1,800,000 for companies.[1]

It is important to note:

- The law does not apply solely to big business. It covers companies that turn over more than $3M as well as government agencies and those that handle health data, regardless of turnover.
- The Privacy Commissioner does not have to consider the impact of a breach purely on the number of records that are exposed. If just a single person suffers significant loss or impact because of a breach, the Privacy Commissioner can act.
- A breach event isn't just defined as customer PII being accessed from outside the business. Just as every employee can play a role in retaining customers, every employee represents a layer of risk when it comes to the misuse or misappropriation of customer PII.

THIS CHURN, IT BURNS!

The cost of a data breach goes well beyond the detection, clean-up and potential fines. The loss of customer confidence can lead to significant customer churn leading to a permanent loss of revenue. Even if a breached company recovers their customer numbers, there may be months or years of lost revenue while customer numbers recover.

In fact, 89% of consumers say they avoid doing business with companies that they do not trust to protect their data. 60% of Australians have eliminated providers because of such concerns[2] , which is testament to how much more educated and aware consumers are about data protections and privacy.

These facts suggest customer retention teams will wear considerably more work because of a reported breach event. The scale of data loss, the speed of customer fall out, the rate of social media spread, the impact on contact centres, executive briefings, planning and deployment of counter measures all equate to a lot of additional work for all affected teams.

To illustrate this, consider a standard model for an electricity provider in Australia with 3.5m customers and a marketing budget of approximately $8m.

- If a breach event resulted in churn of just 0.5% of that base, or 17,500 customers, it would equate to approximately $1.75m in lost revenue annually.
- Depending on the cost of acquisition, approximately $250,000 would be needed in additional marketing budget to recover lost customers.
- $150,000 or more may be required to develop and deploy counter measures to prevent competitors clawing additional customers out of the business because of a breach.

REFRAME TO RETAIN

The good news is that in a mandatory reporting environment, having excellent information security becomes a greater competitive advantage. If customers will avoid businesses they feel cannot be trusted with their data, the converse also true.

Data security is very clearly a matter of customer care, which is why retention teams and business risk managers need to work with IT to ensure the right technologies and processes are in place to reduce the likelihood of a mandatory breach report ever taking place.

The data security technology stack in most organisations is quite complex but there tends to be an overemphasis on solutions that protect against breach from the outside. In fact, in the CSO Oracle Market Pulse survey, 2/3 of security budgets went toward network protections but this spend resulted in less than 1% of detected breaches.

So what can you do?

Understand the role of the insider in creating risk for your customers, and you talk to your business risk and IT colleagues to understand how database and file activity is monitored internally, and what controls are placed on the access to customer data throughout the organisation.

BE TRANSPARENT

Let customers know why you are collecting their data and how it is used. As part of a retention strategy, work with your business risk and IT colleagues to consider where the business could innovate with new processes and products that rely less on the collection and storage of PII. For instance, is it possible to offer a service that the customer controls, where your business only accesses PII on an authorised, as-needs basis?

EDUCATE YOURSELF

Ask questions about the ways your department accesses or utilises customer PII. Ask questions about the monitoring systems that the business uses to let the right people know when data are being accessed in unauthorised or unexpected ways

Work with business risk, IT and your divisional leadership peers to set up correct rules and policies around access to PII for your teams. This helps ensure you are doing all you can to reduce departmental/ divisional liability in the event of a data breach.

TAKE THE LEAD ON PROCESS DISCUSSIONS

Work with business risk managers and IT to identify how many places PII is captured and used, and discover where there may need to be additional separation of duties to prevent unauthorised access or use of those data internally. Find out where customer PII is collected, stored or utilised by 3rd party partners, suppliers or vendors.

ACT SOON

Although the new Bill was passed in February 2017, it has not yet been given Royal Assent. That means it is not yet law. Once that process is complete, which is a formality, businesses will have several months to prepare for the new regulatory regime.

That gives business time to look at their current data protection posture, put in place measures that address their risks and to develop robust response systems and processes to ensure the direct fiscal impact and potential customer churn are addressed.

QUANTIFY YOUR CHURN RISK

Empower yourself to communicate confidently with your IT partners even if you're not an expert in the field of data security. Work with experts who understand the relationship between data security and customer care. Consider an assessment that will help you quantify the business value associated with a potential churn event versus the technology investments the business may need to make to reduce the likelihood of such an event taking place.

Security priorities are a constant concern for IT teams so you are likely to find willing allies who are keen to reframe the discussion of security around competitive advantage, customer care and innovative business practice.

CONVERSATION KICK STARTERS

Here are six questions you should ask of your Technical Risk and IT partners to help understand how your team / function might be exposed by insider threats to your data.

1. Do we use unmasked customer data in tests or training? If so, what are the controls around this?

2. How can I be alerted quickly when one of my team members is accessing data they shouldn't be or in an unusual way?

3. Among the systems used by my team / department, which ones contain sensitive data? How are they protected from possible breach?

4. What contingency budget is in place to cover the additional time and resource my team would need to respond in the event of a data breach?

5. Do we have the ability to monitor and change access to databases and files in real time?

If the answers you're getting are vague or leave you unsure, it's probably time to talk to an expert.

DATA MIGRATORS

We're the people who understand the importance of data in modern organisations. Energy and Utilities? Finance? Road Tolling? Logistics? You're almost certainly a data-driven business. The quality, flow, security and performance of your enterprise data is imperative. Data Migrators has proven that data governance can be done right first time, We're a strong team of experienced professionals who believe it's time to reverse the trend. Keen to help organisations avoid making the same fundamental governance mistakes witnessed time and again, we formed with the express intention of providing the market with one service provider who could ensure data governance success, and demonstrate excellence in operational data management.

Our proven team can make your data governance an exception to the statistic. That's not marketing, it's a fact, and we'd love to meet you to discuss how we can make your data security treatments a success too.

TeamSquare, Level 2,
520 Bourke Street
Melbourne
Victoria 3000
Australia

Call us on **1300 328 264**
Or email us at **enquiries@datamigrators.com**

www.datamigrators.com

REFERENCE

1. http://www.pwc.com.au/legal/assets/legaltalk/privacy-amendment-notifiable-data-breaches-bill-2016.pdf

Data Migrators

IBM Silver Business Partner