CLYDE&CO

INSIGHT

Data breaches – how to effectively avoid them and manage them if they happen

March 25, 2015 | Written by Dean Carrigan and John Gallagher

The risk that often fails to make the list of operational business risks is, arguably, one of the most significant – and that's the risk of a data or privacy breach. As methods of conducting business evolve, and with constantly changing technology platforms for sales and promotion; new media for brand awareness; and new audiences and markets, the risk of a data breach has rapidly increased in severity and exposure. With the extent and nature of the type of information being exchanged between customers and businesses expanding now more than ever before, the time for business to address this risk is now.

Recent awareness

High profile data breaches are the subject of daily chatter. The list of breaches hitting the US market gets longer and longer: Anthem; Target; Home Depot; Neiman Marcus, to name but a few. The financial costs arising from those breaches are very significant, with estimates stretching into the hundreds of millions of dollars.

Proper insurance cover helps manage the financial impact of a data breach. But with reports of businesses being slow to recognise the risk of a breach, and a slow uptake in the market for cyber risk insurance cover in the Asia Pacific region, the likelihood is that many Australian businesses may be left exposed to very significant losses.

2014 saw an increased focus on how Australian businesses handle personal information, and the security of the systems holding that information. Most recently, the Privacy Commissioner has indicated that the responsibility for privacy governance goes all the way to the top – with the CEO, the Executive, the board and the management of any organisation being ultimately responsible for promoting privacy as an asset to be respected, managed and protected.

ASIC, our corporate regulator, is also alive to these issues and has just issued a report highlighting the importance of cyber resilience to ASIC's regulated population.

While the Australian market has not yet experienced a significant data breach, it appears almost inevitable that there will be a significant breach in the future. Experts estimated in 2014 that the average cost of a data breach for Australian organisations is more than AUD 2.8 million per year and rising.

So, are you prepared?

In this article, we consider what you can do to prepare for a data breach and the key steps you need to consider to prepare your business.

Consider and prepare

The type and severity of breaches vary enormously from business to business, dependent on the industry, the method of trading, the organisational structure, etc.

Some breaches are innocent: an employee loses an un-encrypted work phone; a laptop containing personal information is left in the bar at after-work drinks; a confidential email is sent to the wrong recipient. Others are more sinister: an unlocked filing cabinet of medical files is stolen; a malware bug invades your system and destroys or copies files containing personal information; a hacker breaks into your system and steals all personal information held on your files, choosing to sell it to the highest bidder on an anonymous hacker forum.

Knowing and understanding the information your business holds is key to preparing for a breach – what information do you hold and what are the security risks to that information and the consequences of a breach of that security? Some information is more likely to cause harm if it is compromised – *eg* medical records or financial account details – and this requires additional, more secure protection.

Identifying the key areas in your business that could be susceptible to a data breach is the next key step in preparing. What protections are in place to ensure the security of information at each stage of its transition into, through and out of your business?

Consideration needs to be given to the platforms upon which your business operates – is it online; is it direct with the customer or through intermediaries; is it domestic or also offshore? Where is the information stored? Where are the servers based and what protection is afforded to them? How is the server protected? Who manages the security system? Where could there be weaknesses in the information chain?

Once you've completed the initial risk assessment and identified the vulnerable areas of your business, you can devise and implement protections tailored to those risks and suitable for your organisation. These protections should be pro-active as well as re-active.

Key steps to prevent a data breach

- **Reviewing the systems and policies for handling information in place at your business** – how can they be bolstered and improved to reduce the risk to information security?
- **Considering IT systems usage policies** – how is access provided, who can grant access and who controls access levels? Are files encrypted? Who monitors access and copying?
- **Assigning responsibility for information security** – who is the most appropriate person in your business to manage data breaches?
- **Reviewing training and awareness** – are employees and executives trained on an ongoing basis in the content and purpose of your security protocols? Who monitors awareness and execution?
- **Developing a breach response plan** – what needs to be done in the event of a breach, and who does what and when, in a breach scenario? We discuss this key step further below.

By putting suitable arrangements in place prior to a breach, you limit your business' exposure to the risk of a breach in the first place, and enhance its ability to respond in a timely and coordinated manner if a breach does occur. However, it's not possible to eliminate entirely. Therefore, you must prepare and plan for the event of a breach.

React quickly

If your systems are compromised, time will be of the essence. A well formulated and executed breach response plan will, if executed effectively, save your business time; mitigate risk of contagion; and, in the long run, reduce the costs, the reputational damage and overall harm to your business caused by the breach.

Some insurers in the market offer products complete with breach response plans and response teams provided as part of the package. A critical gap exists in the risk and security framework of those businesses that do not have specific data breach cover, or a formalised response plan in place.

Key to formulating an effective plan is an awareness of your business and the vulnerable areas that may be susceptible to a breach. Each breach differs and will need to be handled on a case by case basis.

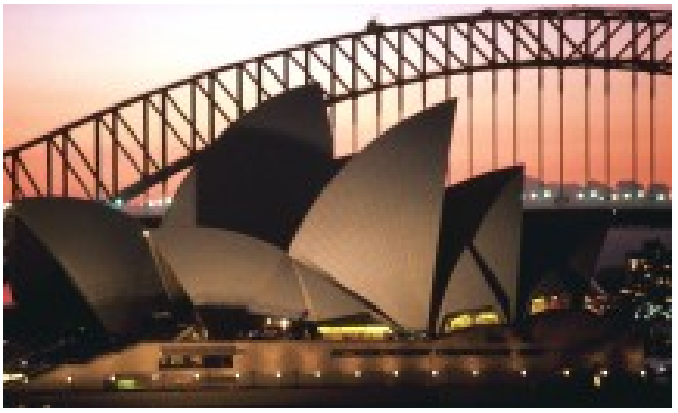
Some key factors to consider in developing a plan

- **What different types of breaches are likely and how must the business react in each case** – what level of lock-down is required to contain a breach? This will depend on a number of factors including: what information has been compromised; the nature/cause of the breach; the systems involved; and the potential for harm to be caused. Often, businesses hold different types of information, each requiring different protection levels – *eg* personal/sensitive/medical/financial information. Each situation is different but all possible scenarios should be considered and the necessary immediate responses clearly mapped out.
- **Who within the business needs to react in the event of a breach** – who are the key figures in your business that must be represented and involved in the response? A typical breach response team will involve specialists in each of IT, risk management, legal and compliance, finance, HR and, (often overlooked) customer relations. It's essential that representatives from each of the relevant aspects of the business are aware of their role in the event of a breach. For example, who has authority to lock IT systems down? Who allocates tasks and leads the investigation?
- **Which external advisors need to be on call** – who are the most appropriate advisors for a breach affecting your business? Typical advisors in the event of a breach include forensic teams, lawyers, PR agencies and IT security experts – each of which play important advisory roles. You should consider a range of advisors and come up with alternatives, where necessary to suit a particular type of breach. Experience of dealing with breaches is key to handling them in an appropriate and effective manner.
- **What notifications are necessary** – do you need to notify customers, law enforcement authorities, regulators, business partners, third party service providers, etc? Who must be notified and how notification should be made will entirely depend on the breach, and the level of information that has been compromised. While we have yet to see mandatory notification requirements in Australia, the Privacy Commissioner's view is that if there's a real risk of serious harm as a result of a data breach, the affected individuals and the OAIC should be notified. So, consideration will need to be given to the different possible scenarios and whether notification may be necessary (and, if so, what type of notification is warranted). Consideration should also be given to whether you have complete and up to date customer contact details to enable a notification.
- **How does the plan evolve** – who is tasked with updating the plan to reflect changes to your business? Is the plan tested on an ongoing basis? What are the post-breach procedures – who reviews the plan after it is used, having regard to any shortfalls that were identified as a result of a breach? Are staff aware of and trained in the plan? Like any policy, a breach response plan should remain live and be reviewed and tested on regular basis to ensure it is fully effective at the time of a breach.

By laying down suitable and secure foundations now, before a data breach occurs, you can better manage the risk of a breach and significantly reduce the losses and reputational damage that a breach may cause. Conversely, a poorly managed, slow, unplanned and/or disorganised breach response has the potential to cause significantly increased losses and damage to your business.

The failure to effectively execute the remedial steps can do more harm than the breach itself. Therefore, a carefully planned breach response strategy should be an integral plank of your risk management and security framework. The need to be alive to the risks facing your business from data breaches has never been more important.

Similar stories



19 DECEMBER, 2014

Corporate Insurance Advent Calendar - Dealing with Big Data cause…

22 OCTOBER, 2014

Legal Update: Paul Sofio v. OCRCVM

02 OCTOBER, 2014

The recent decision of the Supreme Court of Western Australia in…

14 JANUARY, 2015

New era of supervision of Australian private health insurers

16 FEBRUARY, 2015

Cabotage reform in Australia - the 2012 “reforms” and the need for…

On 1 July 2012 the previous Australian Labour Party (ALP) government of Prime Minister Julia Gillard enacted the Coastal Trading (Revitalising…

25 JANUARY, 2012

New Rules on European Data Protection announced

Authors

Dean Carrigan
Partner

John Gallagher
Senior Associate

More by the authors

- Tightening Australia’s foreign bribery laws - amendments presented to…
- Support for crowdfunding in Australia and the implications for insurers
- New era of supervision of Australian private health insurers
- Corporate Insurance Advent Calendar - Regulators to act to reduce underinsurance
- Corporate Insurance Advent Calendar - Dealing with Big Data cause…

Categories

Sectors

Cyber

Services

Commercial | Data Breach, Response & Recovery | Data Protection & Privacy | Data Security | Dispute Resolution | HR Data Management | Insurance | Regulatory & Investigations | Technology

Locations

Asia Pacific | Brisbane | Melbourne | Perth | Sydney