A practical guide to responding to data breaches

It is time to shift your thinking

It is clear that times are changing. There can be no dispute that the conversation regarding privacy and data protection has shifted dramatically from the data room to the boardroom. One of the key features of this shift is that privacy laws and consumers are demanding much more from business and Government when it comes to the protection of data and personal information.

This shift can be a daunting prospect for CIOs and IT Managers responsible for IT systems and infrastructure, as well as CEOs and C-Level Government executives who are accountable to shareholders, consumers, the public and other key stakeholders.

Maddocks and Commvault are committed to providing practical guidance to helping you effectively manage this transition within your organisation.

With so many significant legislative changes on foot, we have stressed that now is the time to review your organisation’s privacy resilience.

In our recent joint fact sheet we outlined our practical Review – Refine – Retest and Respond framework for organisations to assess whether they are ready for the new mandatory data breach reporting obligations (Mandatory Data Breach Laws) under the Australian Privacy Act 1988 (Cth) (the Privacy Act). We have also given you a survival guide for preparing for the introduction of the General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) which may also apply to you.

In this next instalment of practical guidance we explore in more detail the key steps to actually responding to a data breach, or Step four in our Review - Refine – Retest and Respond model, including taking you through a hypothetical scenario.

It is our firm belief that organisations who are robustly prepared and who take a ‘whole of business’ approach to privacy and data protection can move from a place of reaction and fear to a place of confidence and cyber resilience, even in the face of the most serious and stressful data breaches.
Key elements of responding to a data breach

Whether it is a monumental technical issue involving your mission critical IT infrastructure or a one-off isolated incident of accidental mishandling by an employee, each privacy breach will involve different circumstances, and there is no single way to respond.

It is critical for your organisation to have a clearly set out a pre-agreed framework which forms part of your internal systems and processes for responding to data breaches on a case-by-case basis - your Data Breach Response Plan.

Maddocks and Commvault believe that the key elements of responding to a data breach include:

01 Assess + React
02 Notify
03 Review

**Key Tip** Remember that timing is critical, particularly for steps one and two. Delays in completing these steps can expose an organisation to significant financial penalties as well as brand damage and loss of customer confidence. Accordingly, an important step is to ensure all key stakeholders within your organisation are familiar with your internal Data Breach Response Plan before a breach occurs so that they can promptly activate the necessary steps to mitigate potential impacts.
We see time and again, that face-to-face training with employees can be one of the most effective ways to communicate the fall-out from a data breach and the seriousness of the consequences, as well as educating on how to respond to a data breach and the details of your specific Data Breach Response Plan.

Set out below is a worked example of a data breach, followed by some commentary on how this could have been handled better.

**When things go wrong – a breach**

An online organic retailer leading the market in bespoke handcrafted produce has discovered that for the past three months, when customers have been entering their payment details on their website to order goods, these details have been skimmed and are being sent to China and Indonesia and onsold.

The retailer’s CEO was busy meeting organic suppliers of coffee in remote Africa at the time and difficult to contact. Management did not have a direct line of contact to the board of directors outside of the CEO nor authority to sign off on data breach response actions without the CEO.

The retailer was unable to verify how many customers had been affected and whether all payment methods had been compromised. The retailer immediately shut down its payment platform and then engaged an IT specialist to try to trace the hacker.

Due to delays in contacting the CEO and difficulties in assessing the data breach, it took the retailer 12 days from the discovery of the data breach to notify customers via email and separately issue a media statement. A disgruntled customer tweeted prominent media outlets including the email notification to customers. It became clear that the media statement was inconsistent with the email notification to customers.
Assess

Once you become aware that a privacy breach has occurred or is suspected, quick action is crucial to stop the damage becoming worse. We recommend that where possible, you assess and react in parallel.

In order to be able to take effective action, you must understand the nature and scale of the data breach. Ideally an initial assessment of the data breach should be completed as promptly as possible with consideration of applicable mandatory reporting times (which we discuss in more detail in our recent article on the GDPR). In the example on the previous page, there were several issues with the retailer’s initial assessment process:

- the absence of a Data Breach Response Plan and robust policies and procedures caused delays – management were unsure what action they should be taking in such a case and who was appropriately authorised in the absence of the CEO; and
- the retailer had inadequate data retention and access control systems, which meant it was not able to verify how much and what type of personal information had been compromised.

React

Where a data breach occurs, being responsive is vital. However, consideration needs to be given as to whether the proposed action could have adverse consequences, for example by destroying evidence that may be needed later.

In the above scenario the retailer shut down the payment platform before communicating with an IT specialist. In the case of a hacking, alerting the hacker you are aware of suspicious activity will cause them to destroy evidence of the hacking. It is important that you speak to specialists as soon as possible to understand the risks associated with taking certain actions.

As part of the reaction phase, you could also:

- consider any other security measures (e.g. change of passwords or user details, removal of information, recall of emails, limiting access, contacting third party ISPs);
- create a list of all affected people and their contact details;
- consider who else should be notified of the data breach;
- prepare file notes which document all actions taken and the relevant timeframes;
- prepare your plan for notification; and
- consider contacting other key stakeholders such as, the police to investigate the hacking; suppliers to the retailer – for example, the retailer may have obligations to its bank under its merchant/processor agreements to notify in the event of data breach; the retailer’s insurer – cyber security insurance policies may have notification requirements for coverage; and PR agencies to prepare statements and media releases.

To ensure you have appropriately identified the actions that should be taken, it may be necessary to engage with lawyers and other specialists during this phase. They will also be able to assist in the preparation of any notifications required under Mandatory Data Breach Laws or other laws such as the GDPR.
Notify

Once you have an understanding of the nature and scale of the data breach, in some cases you may also be under a legal obligation to notify those affected.

As we have previously outlined, notification is only required in certain circumstances:

- Under the Mandatory Data Breach Laws, if an ‘eligible data breach’ has occurred, both the affected individual(s) and the Office of the Australian Information Commissioner (OAIC) must be notified ‘as soon as practicable’, using a statement which includes certain mandatory information. The specific criteria for an eligible data breach are detailed in our Review – Refine – Retest and Respond fact sheet.

- Under the GDPR, which may apply to your business even if you are not located in Europe, the notification period is 72 hours. You can read more about the specific criteria in our GDPR Fact Sheet.

Again, timing is vital for notification and failure to promptly notify may put you in breach of privacy laws which can result in penalties of up to $2.1 million for corporations in Australia, and four percent of annual global turnover or €20 million (whichever is higher) under the GDPR.

Key Tip Importantly, where data is accessed, disclosed or lost but robust encryption is in place, your organisation will ordinarily not be required to notify the breach.
Review

Once the storm has passed, it is important for organisations to undertake a comprehensive review of its systems and the response to the data breach. This stage is effectively stage one of our Review – Refine – Retest and Respond framework. A review in the case of our worked example might determine that the retailer should be:

- developing a Data Breach Response Plan;
- reviewing security risks to personal information;
- reviewing its contractual arrangements with vendors who handle personal information; and
- undertaking whole of business privacy training so that staff are more adequately prepared.

Once the Review stage has been finalised, ensure you Refine and Retest as outlined in our Review – Refine – Retest and Respond framework.

If you would like to learn more about responding to data breaches or adopting our framework of Review – Refine – Retest – Respond, please contact Commvault or Maddocks.

We can also assist with implementing training and educational programs for your organisation as well as developing Data Breach Response Plans.

Michael Bishop | Commvault
APAC Legal Director
61 2 8243 9815
mbishop@Commvault.com

Brendan Tomlinson | Maddocks
Special Counsel
61 2 9291 6121
brendan.tomlinson@maddocks.com.au

Sonia Sharma | Maddocks
Senior Associate
61 2 9291 6143
sonia.sharma@maddocks.com.au

Elizabeth Lilley | Maddocks
Senior Associate
61 2 9291 6128
elizabeth.lilley@maddocks.com.au