Data breaches sink senior management careers - don't be next

BY DAVID SMITH, PARTNER, GADENS
JUNE 2015

Recently we've seen CEOs and CIOs at major organisations lose their jobs because of data breaches that happened on their watch. Hacking, data theft and accidental data disclosure are risks that continue to grow. How can you ensure your organisation is well prepared in case a data breach occurs?

RECENT DATA BREACHES

When a company suffers a major data breach, questions are raised about the oversight provided by senior management. The fallout from recent breaches demonstrates this (see "Data Disaster" boxes).

The recent breaches highlight that it is not enough for organisations to implement robust IT security measures. Even the best security measures aren't guaranteed to succeed. As databases continue to grow in size and value, hacking and data loss incidents will continue to occur. The large, sophisticated databases that organisations are developing make prime targets for data theft, and make for serious consequences if there's an accidental release of data.

Your organisation needs to go the next step. Apart from just considering how to avoid a data breach, you need to prepare to respond to a data breach if it occurs.

If you're not ready to respond sensibly and very swiftly, a data breach can quickly result in the public losing confidence in your organisation and its ability to manage personal information and customer relationships.

DATA DISASTER #1 – TARGET US

The US retailer Target suffered two enormous data breaches in late 2013. Up to 110 million customers were affected. Around 40 million sets of credit card details were stolen.

Target was criticised for not being quick enough to let the public know about the breach. Phone lines and social media sites were swamped in the aftermath.

Target's share price dropped by close to 20% after the breach and took around 12 months to recover. Target ran full-page apology ads in over 50 newspapers. In March 2014 the company's CIO resigned. In May 2014 the company president/CEO stepped down.

Target is paying significant sums to resolve a class action lawsuit that followed the breach.

AVOIDING A DATA BREACH

There are steps you can take to reduce the risk of a data breach occurring and to reduce the impact if a breach does occur.

- Conduct an audit to identify your principal security risks and the likely impact if a breach occurs. Then put measures in place to mitigate risks that are likely and/or would have severe consequences if they occur.
- Ensure that your audit also covers risks associated with third party service providers who store or process data for you. The Commonwealth Privacy Commissioner expects organisations to be pro-active in managing privacy risks relating to their service providers. In many cases an organisation will remain effectively responsible under the Australian Privacy Principles for a data breach if its service provider did not take reasonable security steps.
- When you put personal information into the hands of a third party service provider, ensure you put suitable privacy and security clauses into your agreement and take steps to monitor the service provider's compliance with the agreed security regime.
- Put clear internal policies in place around privacy, security and fraud awareness. Train your staff regularly on these policies.

- Delete personal information you no longer need. Australian Privacy Principle 11.2 also gives you the option of de-identifying it, but after a recent landmark determination by the Privacy Commissioner (see our article here) it appears that even de-identified data may still sometimes be personal information, so you may have ongoing privacy law obligations even after de-identifying the data. Certain recent data breaches in Australia have highlighted that organisations are not always good at deleting or de-identifying personal information once they no longer need it.
- Engage suitable third parties to test your data security regime.

BEING READY TO RESPOND TO A DATA BREACH

Hopefully you'll never face a serious data breach. But if you do you'll need to be ready to respond very quickly and sensibly. You should develop a Data Breach Response Plan now, so that you're ready to respond straight away if an incident occurs.

We recommend that you designate a single position within your organisation with responsibility for data security and developing and maintaining a Data Breach Response Plan. Commonly this is the Chief Technology Officer.

You should also designate a team of people who will manage any data breach response. If an incident occurs, your organisation needs to be clear about who is responsible for managing the response. The team should comprise senior managers such as the Chief Technology Officer, the Privacy Officer and representatives of the legal, public relations and HR teams.

DATA DISASTER #2 – KOREAN BANKS

In early 2014 an employee from Korea Credit Bureau stole information relating to about 20 million debit and credit card holders and sold it on to marketing companies. In the fallout, the CEOs of the three affected Korean card issuing banks resigned.

Immediately after the incident was announced, card holders were frustrated when the banks' websites and call centres were overwhelmed and long queues formed in branches.

Include the following in your Data Breach Response Plan:

- A checklist to follow in order to understand the nature and extent of the data breach, to understand its cause, to contain the breach and to preserve the evidence.
- A framework for evaluating the risks flowing from the breach. What is likely to happen to the data the subject of the breach? Is any other data in immediate danger?
- Guidance on how to decide whether to notify the affected individuals and the Privacy Commissioner. It is not currently mandatory to report a data breach, although the law may be changed later this year to make it mandatory. At the moment the Privacy Commissioner recommends you notify an individual if the breach creates a real risk of serious harm to him/her. A serious data breach should also be reported to the Privacy Commissioner (although again, this is not currently mandatory). Plan for how you will notify individuals. If you do have to notify, consider sending hard copy letters because email messages of this type may be mistaken for spam or "phishing" emails. Include a template letter in your Data Breach Response Plan.
- Instructions on how communications with the media, the general public and your business partners should be handled. Do you have any contractual obligations that require you to notify business partners? How will you quickly put 1800 numbers and web pages in place if needed to respond to a large volume of queries?
- A checklist to follow to determine what changes you need to make to prevent further breaches. Possibilities might include improving security, additional training for staff and changes to data collection, storage or processing practices. Changes to your recruitment process, internal privacy and security policies, and agreements with third parties might also come into consideration.

- A list of contact details for people you may need to contact quickly. This might include your key customers, service providers who help you to store or process data, police, regulators in your sector and external lawyers and public relations advisers. Your insurers and key business partners should also be added to the list.

Develop your Data Breach Response Plan so that it's consistent with, and part of, your organisation's broader crisis management framework.

Treat risk management as an ongoing task and not a "set and forget" proposition. You need to continually review your risk profile and the measures you have in place to manage risk.

DATA DISASTER #3 – STATE OF UTAH

The public sector is not immune. In 2012 the IT infrastructure of the State of Utah was hacked and personal data, including social security numbers, of nearly 800,000 people were taken.

The Governor of Utah apologised for the failure to protect the personal information and fired the state CIO.

FURTHER INFORMATION

There is more information about how to prepare for and respond to a data breach in the Privacy Commissioner's Guide to Handling Personal Information Security Breaches.

While nobody expects a data breach to happen at their organisation, these things do happen to some organisations. Whether you have a good Data Breach Response Plan in place may make all the difference between a manageable outcome and an outcome that is very bad for the organisation and its senior management.

CONTACT DETAILS

David Smith
Partner, Melbourne
Intellectual Property and Technology

T +61 3 9252 2563
E david.smith@gadens.com