Data Breach Plan – Responding to a Data Breach

2020 has seen the COVID-19 pandemic drive overwhelming societal and organisational changes, such as challenges for cyber security and data theft. It has seen the continued disruption for many government agencies and enterprises, and has fundamentally changed the way they do business. As the backbone of the Australian economy, it is imperative that government agencies and enterprises not only adapt and recover, but are also set up for success in the next normal future. This will require extraordinary flexibility, coordination, adaptability and resilience during what may be a prolonged period of recovery, uncertainty and change.

In response to these challenges IIM has created this resource on the topic of "Data Breach Plan – Responding to a Data Breach".

A Data Breach Plan should consider the following:

- How to contain the data breach
- Evaluate the associated risks
- Consider if you need to notify affected individual(s)
- Consider if you need to notify appropriate statutory bodies or other impacted organisations
- Put in place preventative actions for example preventing a repeat by documenting lessons learnt

Data Breach Plan - Evaluate Risk

To determine what other steps might be needed, you should identify the type of data involved in the breach and assess the risks associated with the breach. Factors to consider could include:

- What type of data is involved?
- Who is affected by the breach?
- What was the cause of the breach?
- What is the foreseeable harm to the organisation if the data breach was the theft of company sensitive information?
- What is the foreseeable harm to the affected individual(s) if the data breach was the theft of personal information?

Data Breach Plan – Preventative Actions

Produce a data breach report and include recommendations on how to prevent any further reoccurrence. Your data breach report might include the following preventative activities:

- Undertaking a security audit of both physical and technical security measures and controls
- Reviewing data protection, governance policies and any other policies and procedures that cover storing, protecting, security and privacy of data including the handling of personal data.
- Reviewing employee training procedures and practices
- Reviewing contractual obligations especially data protection clauses with contracted service providers and contractors.

Data Breach Plan – Seven Steps

Step 1:	How do data breaches occur?
Step 2:	Data breach management and notification process
Step 3:	How to contain the breach
Step 4:	Evaluate the associated risks
Step 5:	Consider if you need to notify affected individual(s).
Step 6:	Consider if you need to notify appropriate statutory bodies or other impacted organisations.
Step 7:	Put in place preventative actions for example preventing a repeat by documenting lessons learnt.

Data Breach Plan – Step 1 How do data breaches occur?

Data breaches can occur in a number of ways for example:

- lost or stolen laptops, removable storage devices, or paper records containing sensitive company information and/or personal identifiable information
- databases containing sensitive company information and/or personal information being illegally accessed
- failure to comply with statutory regulations on data protection and/or privacy
- employees or individuals accessing and disclosing sensitive company information and/or personal information outside of the authorisation of their job position
- employees or individuals mistakenly providing sensitive company information and/or personal information to the wrong person
- paper records stolen from insecure recycling or garbage bins
- hard disk drives, multifunction printers or databases being disposed of without the contents being erased

Data Breach Plan – Step 2 Data breach management and notification process

Your agency/enterprise should have a clear data breach plan in place. The data breach plan should identify the key responsible personnel, who should be notified and set out the procedures for identifying how to respond to the data breach. The data breach plan should consider some of the following:

- how to contain the data breach
- evaluate the associated risks
- consider if you need to notify affected individual(s).
- consider if you need to notify appropriate statutory bodies or other impacted organisations
- put in place preventative actions for example preventing a repeat by documenting lessons learnt

Data Breach Plan – Step 3 How to contain the breach.

Take whatever steps are needed to contain the data breach and minimise any potential damage to the organisation. For example, take all possible actions to recover the data, shut down the system that has been breached and suspend the activity that lead to the data breach. If a third party is in possession of the data and refuses to return it, you may need to seek legal advice on what action can be taken to recover the data.

When recovering the data, take all steps possible to make certain that copies of the data has not been made. If copies of the data have been made take all precautions possible to have these data copies recovered.

Be careful when taking steps to contain the breach not to destroy any information that may be needed to investigate the cause of the breach.

Data Breach Plan – Step 4 Evaluate the associated risks.

To determine what other steps might be needed, you should identify the type of data involved in the breach and assess the risks associated with the breach. Factors to consider could include:

- what type of data is involved?
- who is affected by the breach?
- what was the cause of the breach?
- what is the foreseeable harm to the organization if the data breach was the theft of company sensitive information?
- what is the foreseeable harm to the affected individual(s) if the data breach was the theft of personal information?

Data Breach Plan – Step 5 Consider if you need to notify affected individual(s).

As part of your evaluation of the data breach you will need to consider if you need to notify affected individual(s). In general, if a data breach creates a risk of harm to an individual, the affected individuals should be notified.

Prompt notification to individuals in these cases can help to avoid or lessen the damage by allowing the individual to take steps to protect themselves. Failure to notify affected individuals of the data breach may compound the damage for the individuals affected and reflect negatively on an organisation's reputation. Notification in these cases can exhibit a commitment to open and transparent governance.

Note: Care should be taken. There are occasions where notification of a data breach to an individual can be counter-productive. For example, notifying individuals about a privacy breach that is unlikely to result in any adverse outcome for the individual might cause unnecessary anxiety. In either of these example cases you may wish to seek legal advice on how best to address the identified breach.

Data Breach Plan – Step 6 Consider if you need to notify appropriate statutory bodies or other impacted organisations.

As part of your evaluation of the data breach you will need to consider if you need to notify appropriate statutory bodies and/or other possibly impacted organizations.

In general, if a data breach creates a risk of harm to the government or another organisation then you should identify any mandatory data breach notification regimes.

In this type of data breach, you should seek legal advice on how best to respond to this type of data breach.

Data Breach Plan – Step 7 Put in place preventative actions for example preventing a repeat by documenting lessons learnt.

Once the data breach has been contained, you should undertake further investigate to identify the circumstances of the data breach and determine all relevant causes.

An outcome of this analysis should be documented and any lessons learnt should be incorporated into your data breach report. Your data breach report should also include recommendations on how to prevent any further reoccurrence. Your data breach report might include the following preventative activities:

- undertaking a security audit of both physical and technical security measures and controls
- reviewing data protection, governance policies and any other policies and procedures that cover storing, protecting, security and privacy of data
- reviewing employee training procedures and practices
- reviewing contractual obligations especially data protection clauses with contracted service providers and contractors.

For Further Information on Notifiable Data Breaches

For further information go to the Australian Government Website for Notifiable Data Breaches scheme at:

https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme

---

FOR MORE INFORMATION CONTACT:

Institute for Information Management Ltd. (IIM)
Email: iim@iim.org.au
PO Box 4195, Balwyn East, Victoria, 3103 Australia
(03) 5424 8551