TECHNOLOGY 360

Data Breach Response Plan

Prepared by Chris Freeman

Technology 360 Group

Date 20th June 2018

Version 1.0

Purpose of the document

This Data Breach Response (DBR) plan sets out clear escalation procedures and pathways of authority for Technology 360 Group staff in the event that a data breach has occurred or suspected to have occurred.

The purpose of this document is to enable the Technology 360 Group team to respond quickly to a data breach and reduce the impact of any such breach on clients (either at the organisational or individual level).

What is a data breach?

A data breach is the unauthorised access, use or disclosure of one's personal data without their consent. Data breaches can be knowingly or unknowingly caused such as human error, system error, malicious action, lack of security and data protection, and or any other action which may result into serious consequences. Section 6 of the Privacy Act 1988 (Cth) defines a data breach as “lost or subjected to unauthorised access, modification, use or disclosure or other misuse”.

The Privacy Act defines personal information as “information or an opinion about an identified individual, or an individual who is reasonably identifiable”. Different types of personal information can include, sensitive information such as information or opinion about individual’s racial or ethnic origin, political opinion, religious beliefs, sexual orientation or criminal record, provided the information or opinion otherwise meets the definition of personal information; health information; credit information; employee record information and tax file information. It is also important to note that what the Privacy Act doesn’t explicitly recognise as personal information, may be considered personal information under other legislation.

Examples of data breach:

- Stolen personal information by an unknown party due to lack of security measures in place.
- Losing or misplacement of files, or devices, containing personal information.
- Unauthorised access of personal data by staff or other members.
- Carelessness causing devices containing personal information to be unattended.

- Knowingly, or unknowingly, disclosing personal information internally within the organisation or to a third party.
- Not complying with state or federal privacy laws of Australia

Consequences of data breach can be severe as it may result in identity theft, financial loss, defamation, damaging of personal and/or work relationships, effect on mental health, etc.

This plan sets out the roles and responsibilities of staff, lines of authorities, and the process to be followed in the event of an actual, or suspected, data breach with the intention that actions can be taken quickly to minimise the consequences caused by a data breach.

Roles and Responsibilities

Roles and responsibilities of staff when a data breach is discovered or suspected

- Data breach is suspected or notified.
- Data breach is documented, including the following:
    - Affected individual/s
    - Type of the personal information involved
    - Date and time of the breach
    - Potential damage the breach might have already caused
    - Potential damage the breach could cause in the future
- Immediately notify the Board and all senior management staff of the suspected data breach with above details.

Roles and responsibilities of the Senior Management Team when a data breach notification is received

- Determine whether the data breach has actually occurred
    - Enlist any resources required to investigate and confirm a data breach has occured.
- Assess the severity of the data breach and who should manage the data breach.
- The Senior Management Team will determine whether the data breach requires escalation to the Data Breach Response Team (DBRT). The following factors will be taken into consideration:
    - Number of individuals affected by the breach
    - Nature of the breach and types of information breached
    - Reason for the breach
    - Steps required to resolve and / or prevent the breach from occuring again
    - Severity of the damages that the breach has or might cause affected individuals

- Based on the outcome of above analysis, the Senior Management Team may or may not escalate the breach to the DBRT.
    - Regardless, the Senior Management Team will document the breach, the reason for escalating or not escalating to the DBRT, actions taken, changes made, outcomes achieved etc. This report needs to be sent to the DBRT for their analysis and records.

Roles and Responsibilities of a Data Breach Response team

The Data Breach Response Team (DBRT) will typically include:

- A team leader (central point of contact)
    - has the responsibility to manage all incoming data breach requests and report back to senior management.
    - responsible for managing the team and getting their involvement in resolving the data breach.
- A senior member of staff
    - has the responsibility for investigating and co-ordination
    - steps in for the team leader, if the privacy breach is reported by the team leader.
- Head of Customer Success team
    - assists with assessing the risk and ramifications
    - assists with any customer related communications or dissemination of information.
    - takes responsibility for all communications internally and externally with regards to the data breach.
- The HR manager
    - involves and liaises with staff as necessary if requested by the data breach response team, for example, in the occasion of breach caused due to the actions of a staff member.
- Legal representative
    - provides advice and support as required

Each data breach reported to the DBRT are dealt on a case by case basis. Some precedents may be followed if similar breaches have been encountered previously. However, all breaches will be treated as unique with no assumptions made.

The standard steps that the DBRT will follow for any breach include:

- Breach is lodged with the team leader.
- The team leader then escalates the
- Analyse logging - attempt to detect times and sources of breaches (if possible).
- Document timeline of breach including when the vulnerability surfaced, when evidence shows it was first exploited, when it was closed
- Identify how much data was exposed in the breach (worst case)
- Document requirements to fix vulnerability - implement immediately as part of the process if possible
- Investigate related services for similar instances of vulnerability
- Automate password resets where authentication information was compromised
- The team leader then liaises with the Head of Customer Success to communicate the breach to the client/ individual if required. The Head of Customer Success to follow Appendix B while advising the affected individuals.
- The team leader also reports to the Senior Management Team on the following topics using the Formal Report Template at Appendix A. Topics can include:
    - Details on the breach
    - What caused the breach i.e. internal process flaw, human error, system error or as notified by the director
    - Types of information involved
    - Individuals affected
    - Harm caused to the individuals
        - Notifications given, or not given, to individuals affected
    - Actions taken to remedy the breach and minimise the damage done
        - Learnings from the incident
        - What steps put in place to ensure that it doesn't happen again

Appendix A: Data Breach Report

Details on the breach	
What caused the breach- internal process flaw, human error, system error or as notified by the director	
Type of information involved	
Individuals affected	
Harm caused to the individuals	
What notifications have been sent to affected individuals (if any)	
Actions taken to remedy the breach and minimise the damage done	
Learnings from the incident	
What steps have been put in place to ensure that it doesn't happen again	
Other comments from the response team	

Name of response team member involved in managing the breach incident	
Signature	
Date	

References

- Privacy Act 1988
- https://www.oaic.gov.au/agencies-and-organisations/guides/what-is-personal-information
- https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response
- https://www.oaic.gov.au/resources/about-us/corporate-information/key-documents/data-breach-response-plan.pdf

Appendix B: Data Breach - Advice for individuals if they believe they've been affected by a data breach.

Bank details

- If you are concerned your bank details may be compromised, contact your bank and tell them what has happened
- You should also immediately change your account passwords and change your PIN
- Monitor your bank account transactions online and contact your bank if you see any purchases you did not make

Contact details

- Change your email account passwords
- Enable multi-factor authentication for your email accounts if possible
- If you are concerned your drivers licence details have been compromised contact your state transport department and let them know what the issue is
- If it's your Australian passport details you are concerned may have been compromised contact the Department of Foreign Affairs and Trade
- If you are concerned your Medicare details may have been compromised contact the Department of Human Services

Tax file number

- If you suspect your tax file number might be involved in a data breach contact the Australian Taxation Office

Credit report

- You can also ask for a copy of your credit report to check it is accurate. The report shows which organisations have recently checked your credit history, so you can tell them not to authorise a new account in your name
- You can contact credit reporting bodies to place a ban period on your credit report. This means they will not be able to share your credit report with credit providers without your consent for 21 days (unless extended)
- The credit reporting bodies in Australia are:
- Equifax — 138 332
- illion — 13 23 33
- Experian — (03) 8622 1600 or email: creditreport@au.experian.com
- Compuscan Australia — (02) 8404 4217
- Tasmanian Collection Service — email enquiries@tascol.com.au

Online vigilance

- Update any anti-virus software installed on your devices
- Avoid opening attachments from strangers in emails or social media

Report your concerns to authorities

- If you haven't been notified of a breach, but suspect your personal details may have been compromised, report your concerns to local police. Make sure you ask for a police report or reference number to evidence you have reported the issue.
- You can report the suspected breach to the Australian Cybercrime Online Reporting Network (ACORN)
- While for specialist advice you can contact IDCARE, Australia's national identity and cyber support service, who can connect you with a specialist identity and cyber security counsellor for expert advice
- You can also apply for a Commonwealth victims' certificate which helps support your claim that you have been the victim of a Commonwealth identity crime. You can present the certificate to government agencies or businesses to re-establish your credentials or remove fraudulent transactions from their records. Read more on the Attorney-General's Department website.