Data Breach Response Plans:

Effective and responsive plans – building public confidence

Report No. 4 to the Queensland Legislative Assembly for 2022-23

Copies of this report are available on our website at www.oic.qld.gov.au and further copies are available on request to:

Office of the Information Commissioner
Level 7, 133 Mary Street, Brisbane, Qld 4000
PO Box 10143, Adelaide Street, Brisbane, Qld 4000

Phone +61 7 3234 7373 or Freecall 1800 OIC QLD (1800 642 753)
Email administration@oic.qld.gov.au
Web www.oic.qld.gov.au

ISBN: 978-0-6456316-2-3

June 2023

Speaker
Parliament House
George Street
Brisbane QLD 4000

Dear Speaker

I am pleased to present 'Data Breach Response Plans: Effective and responsive plans – building public confidence.' This report is prepared under section 135 of the *Information Privacy Act 2009* (Qld).

The report presents the results of a survey about data breach response plans in 107 responding government agencies.

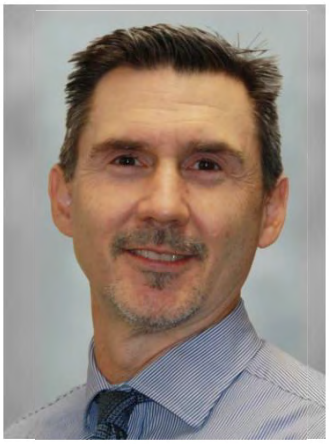
In accordance with subsection 193(5) of the *Information Privacy Act 2009* (Qld), I request that you arrange for the report to be tabled in the Legislative Assembly.

Yours sincerely

Paxton Booth
Acting Information Commissioner

Table of contents

Preface



Data breaches are a significant feature in the privacy landscape. We have seen the impact that breaches have had on the victims of cyber-attacks. They undermine public trust in the capacity of government organisations to safeguard and protect the valuable personal information they hold for members of the community.

Trust in government agencies is vitally important to ensure the community engage with the important functions undertaken by government agencies. The community entrust government agencies with their personal information and expect government agencies to keep it safe. Unfortunately, this trusting relationship can be disrupted by malicious actors who revel in breaking through systems protections and taking other people's personal information for their own gain. Personal information can also be lost through error.

Agencies must strengthen their systems against attack or mishap. They must also plan for a quick and effective response if a breach occurs.

A good agency response will use swift and targeted communication within the agency and with people affected in order to resolve the breach and minimise harm. A data breach response plan assists agencies to achieve these outcomes.

Our Privacy Team works with Queensland government agencies to support their efforts to safeguard personal information. The Office of the Information Commissioner welcomed the Government's commitment to implement the recommendations from Professor Peter Coaldrake's report '*Let the sunshine in',* including the introduction of a mandatory data breach response scheme.

In order to get ready for a more rigorous regime, we surveyed agencies to understand their preparedness for a mandatory data breach reporting scheme.

This survey follows up work started in 2018-19 when we asked agencies about their readiness and documented process for managing privacy breaches, described in our report '*10 years on*'.[1]

Around half of the agencies in our jurisdiction responded to the current survey, and around half of those had a data breach response plan. Most agencies with a data

1 *10 years on: Queensland government agencies' self-assessment of their compliance with the Right to Information Act 2009 (Qld) and the Information Privacy Act 2009 (Qld)*, Report No. 5 to the Queensland Legislative Assembly for 2018-19 - available at www.oic.qld.gov.au.

breach response plan had addressed most of the elements that would make the plan effective. We will continue to work with agencies to build effective data breach response plans.

In the meantime, agencies seeking a better understanding in anticipation of the new scheme can refer to the survey questions appended to this report, or to the Office of the Australian Information Commissioner's *Data breach preparation and response: A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth)*.

It is good practice for agencies to plan to prevent data breaches and respond quickly and effectively if a data breach occurs. Ideally, agencies would publish information about their plans to build community confidence and trust in government.

I commend agencies who are working in this area, and look forward to supporting and working with all agencies to create a secure environment for Queenslanders' personal information.

Paxton Booth

Privacy Commissioner

Executive summary

The increasing frequency and the high impact of data breaches mean organisations need to allocate sufficient time, attention and resources to prevent and manage data breaches.

Government agencies are not immune to the risk of data breaches. Queenslanders entrust government agencies with their personal information. To maintain this trust, agencies need to handle personal information appropriately, and implement strategies to protect it.

All agencies should have appropriate governance and risk management arrangements in place to be able to respond quickly to a breach. A comprehensive data breach response plan can help limit the consequences of a breach, including the risk of harm to the individuals whose privacy has been breached. An effective and timely response to a data breach can help preserve the community's confidence in the agency.

In July 2022, the Queensland Government accepted the recommendations from the Coaldrake review. This includes a recommendation about establishing a mandatory data breach notification (MDBN) scheme for government agencies. Similar schemes operate in other jurisdictions.

We asked government agencies to complete a survey about their data breach response plans in anticipation of a MDBN scheme in Queensland. The survey is based on the Office of the Australian Information Commissioner's *Data breach preparation and response - A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth)*.[2]

The survey prompted agencies to reflect on the systems they have in place to respond to data breaches. We received 107 responses. This report presents the results of the responding agencies' self assessments.

Conclusions

All Queensland government agencies should be alert to the introduction of a MDBN scheme. They should assess their ability to respond to and report a data breach.

The first step for agencies to be ready for the introduction of a MDBN scheme is to have a comprehensive plan for dealing with data breaches. The survey results indicate that there is more work to do before a scheme commences in Queensland.

2 Available on www.oaic.gov.au.

Results

About half the responding agencies said they have a documented data breach response plan. It does not mean agencies are not managing the risk of data breaches or meeting their obligations to protect personal information. A documented response plan is only one element of a broader framework that includes internal controls and strategies to prevent, detect and respond to breaches.

The answers of the 52 responding agencies with a documented data breach response plan indicate some plans are more comprehensive than others. For example, all 52 said their plans outline roles and responsibilities and who to inform if staff suspect a data breach, but only 37 agencies give examples of data breaches to ensure employees understand the diverse types of incidents that they may have to respond to.

Most agencies (42) reported they had established a response team. This can help responding to data breaches quickly and more effectively.

We identified three points for consideration about how the MDBN scheme might operate in Queensland:

- should smaller agencies be able to rely on shared services or larger host agencies to respond to a data breach?
- does the relationship between privacy breaches and data breaches need further clarification?
- are there opportunities to streamline reporting responsibilities in relation to cyber incident reports and reports on privacy or data breaches?

When the Queensland MDBN scheme is launched, the Queensland government may clarify these points, for example in specific sections in an Act or regulation.

Recommendation

We recommend that all agencies have appropriate systems in place so they can prevent and respond to data breaches quickly and effectively.

Systems include policies, procedures, plans and strategies. They form part of an agency's governance and risk management framework.

1 Context

1.1 Definitions

The *Information Privacy Act 2009* (the Act) does not define the terms 'privacy breach' or 'data breach'. While they relate to each other, they also differ slightly. For this report, we use these terms according to their ordinary meaning.

A **data breach** is when data is shared, disclosed or accessed without authorisation, or is lost. An organisation that is the victim of a data breach does not always know, at the time it detects or is told of the breach, what data has been compromised. The organisation may have to investigate to determine whether personal information has been released or accessed without authorisation.

Personal information is defined in the Act as:

> *information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.*[3]

When a data breach involves personal information, it is more likely to affect a greater number of individuals, and will likely be a privacy breach under the Act. Depending on the nature of a data breach, the jurisdiction in which it occurs and whether it meets certain criteria, the breach may attract reporting obligations. We discuss reporting data breaches under various schemes in Chapter 2.

A **privacy breach** can happen when personal information is accessed, used or disclosed without authorisation or is lost, or otherwise dealt with in a way that would not comply with the Act. This may result from a data breach. However a privacy breach is not necessarily a data breach. For example, a privacy breach can occur if an agency does not give sufficient notice to a person about collecting their personal information.

A data breach or privacy breach may be intentional or inadvertent.

1.2 Impact

Recent known data breaches affected millions of Australians: Optus in September 2022, Medibank in October 2022 and Latitude Finance in March 2023. These breaches were the result of malicious attacks.

3 *Information Privacy Act 2009* (Qld), section 12.

Figure 1 illustrates how quickly an apparently 'low risk' data breach can become a major privacy breach. On 14 October 2022, Medibank reported no customer data was accessed. On 9 November 2022, less than four weeks later, the hackers published customers' sensitive medical information online.

Figure 1 – Timeline of Medibank data breach

Date	Progress of Medibank data breach
September 2022	The hackers claim they obtained access to the data using 'jump servers' – a device that allows authenticated users to access a secure system through its firewall.
13 October 2022	Medibank notices unusual activity and shuts down networks.
14 October 2022	Medibank reopens the networks, stating that there is no evidence customer data was accessed.
19 October 2022	The hacker contacts Medibank, claiming to have stolen 200GB of customer data and seeking payment.
20 October 2022	Medibank confirms the claim is legitimate. The Australian Federal Police starts an investigation.
7 November 2022	Medibank confirms the data of 9.7 million past and present customers was stolen.
9 November 2022	The hacker releases customer data on the dark web, including information about a select group of high profile individuals receiving treatment for drug or alcohol use, or mental health disorders.
10 November 2022	The hacker releases more customer data files on the dark web and demands US$10 million to stop releasing data. Medibank refuses to pay any ransom to the hacker.

Source: Cyber Security Hub article, November 2022

Government agencies are not immune and have experienced major data breaches involving personal information.

For example, major breaches occured at:

- ProctorU, a service providing online exams to remote students – records of 444,000 students at Australian universities. (2020).[4]
- Australian National University – records of 200,000 students including the most sensitive financial records such as bank account details. (2019).[5]
- Service NSW, a one stop shop for government services like drivers' licence renewals, a working with children check, registering a birth, or getting a seniors card – 5 million documents, 10% of which contained sensitive data affecting 104,000 people. (2020).[6]
- Ambulance Tasmania – intercepting data transmitted by radio, including patient details for every resident that requested an ambulance between November 2020 and January 2021. (2021).[7]
- Queensland University of Technology (QUT) –personal information of 11,405 past and present employees and students, including their sensitive financial information. (2023).[8]
- QIMR Berghofer, a medical research institute – breaching data held by a third party national data processing company, including personal information for 1128 people. (2022).[9]

Impact on individuals

The Office of the Australian Information Commissioner (OAIC)'s guide to preparing for data breaches describes the impact a data breach may have on individuals:

> *Individuals whose personal information is involved in a data breach may be at risk of serious harm, whether that is harm to their physical or mental well-being, financial loss, or damage to their reputation.*[10]

Medibank's half-yearly report illustrates the potential scale of the impact on individuals. It stated it operated a customer support program, with additional support for customers

4 11 Biggest Data Breaches in Australia (Includes 2022 Attacks), Edward Kost, UpGuard, updated 4 May 2023.
5 11 Biggest Data Breaches in Australia (Includes 2022 Attacks), Edward Kost, UpGuard, updated 4 May 2023.
6 11 Biggest Data Breaches in Australia (Includes 2022 Attacks), Edward Kost, UpGuard, updated 4 May 2023.
7 11 Biggest Data Breaches in Australia (Includes 2022 Attacks), Edward Kost, UpGuard, updated 4 May 2023.
8 QUT, *Cybersecurity incident, Media release – February 6 2023*, https://www.qut.edu.au/additional/cybersecurity-incident.
9 QIMR Berghofer, *Media Statement – QSKIN Study Datatime Breach 2022*, https://www.qimrberghofer.edu.au/news/media-statement/.
10 Office of the Australian Information Commissioner, *Data breach preparation and response: A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth) – July 2019*, page 8, https://www.oaic.gov.au/__data/assets/pdf_file/0017/1691/data-breach-preparation-and-response.pdf.

who called Medibank, fielding 60,000 telephone calls through its Cyber Response hotlines and 13,000 interactions through its Cyber Response Support Program.

Impact on the organisation

OAIC's guide to preparing for data breaches describes the impact a data breach may have on organisations:

> *A data breach can also negatively impact an entity's reputation for privacy protection, and as a result undercut an entity's commercial interests. As shown in the OAIC's long-running national community attitudes to privacy survey, privacy protection contributes to an individual's trust in an entity. If an entity is perceived to be handling personal information contrary to community expectations, individuals may seek out alternative products and services.*[11]

When a government agency suffers a data breach or a privacy breach, this can also affect community trust in government.

In its half-yearly report Medibank said it lost 13,000 policy holders and described the financial impact of the breach:

> *Investment income grew to $55.9 million but was offset by $26.2 million of non-recurring costs associated with the cybercrime event.*[12]

Medibank may incur further costs if the external investigations result in legal or regulatory penalties.

The increasing frequency and demonstrably high costs of data breaches mean agencies need to ensure they are allocating sufficient time, attention and resourcing to preventing and managing data breaches.

11 Office of the Australian Information Commissioner, *Data breach preparation and response: A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth) – July 2019*, page 8, https://www.oaic.gov.au/__data/assets/pdf_file/0017/1691/data-breach-preparation-and-response.pdf.

12 Medibank Newsroom, *2023 Half Year Results - A solid result with business momentum returning - 23 February 2023*, https://www.medibank.com.au/livebetter/newsroom/post/2023-half-year-results-a-solid-result-with-business-momentum-returning

2 Reporting data breaches

2.1 Introduction

Preparation to prevent and manage a data breach is a risk management activity. The Austalian Cyber Security Centre and Queensland Government Enterprise Architecture have guidelines on managing cyber security incidents adopting a risk management framework. Figure 2 presents various aspects of managing a data breach.

Figure 2 – Data breach preparation and response framework

Source: National Institute of Standards and Technology (NIST) Framework, US Department of Commerce

A comprehensive data breach response plan helps an organisation respond quickly and effectively. Reporting a data breach is part of the response phase.

2.2 Anticipating a Mandatory Data Breach Notification scheme in Queensland

Currently, there is no mandatory data breach notification (MDBN) scheme specific to Queensland government agencies. However, Cabinet endorsed such a scheme in July 2022.[13]

13 Premier and Minister for the Olympics, The Honourable Annastacia Palaszczuk, Deputy Premier, Minister for State Development, Infrastructure, Local Government and Planning and Minister Assisting the Premier on Olympics Infrastructure, The Honourable Dr Steven Miles, *Media statement - Taskforce to implement Coaldrake recommendations - 04 July 2022*, https://statements.qld.gov.au/statements/95617.

In early 2022, the Premier announced an independent review into culture and accountability in the Queensland public sector. The reviewer, Professor Peter Coaldrake AO, reported in June 2022.

Professor Coaldrake made 14 recommendations about a range of matters affecting integrity and accountability in the Queensland public sector. In the context of '*Strengthening the underpinning system*', he defined MDBN:

> *Mandatory Data Breach Notifications (MDBN) impose an obligation on an agency to advise an individual if their private information is disclosed, or lost.*[14]

Professor Coaldrake recommended that:

> *Citizens' privacy rights be protected by implementation of mandatory reporting of data breaches. (Recommendation 10)*[15]

Queensland's Premier accepted all the Coaldrake report's recommendations, stating:

> *"I don't just welcome it - I embrace it."*
>
> *"We will accept all of his recommendations and we will implement them lock, stock and barrel."*
>
> *"They are bold, they are comprehensive and they are visionary and they are exactly what I want."*
>
> *"Once they're implemented, Queensland will have the most transparent and accountable government in Australia."*[16]

In 2020, the Crime and Corruption Commission reported on its Operation Impala, a corruption investigation examining Queensland public sector agencies' management of confidential information.[17]

14 Professor Peter Coaldrake AO, *Let the sunshine in: Review of culture and accountability in the Queensland public sector, Final report, 28 June 2022*, page 66 https://www.coaldrakereview.qld.gov.au/assets/custom/docs/coaldrake-review-final-report-28-june-2022.pdf.

15 Professor Peter Coaldrake AO, *Let the sunshine in: Review of culture and accountability in the Queensland public sector, Final report, 28 June 2022*, page 3, https://www.coaldrakereview.qld.gov.au/assets/custom/docs/coaldrake-review-final-report-28-june-2022.pdf.

16 Premier and Minister for the Olympics, The Honourable Annastacia Palaszczuk, *Media statement - "Lock, stock and barrel" Premier embraces Coaldrake Review - 28 June 2022*, https://statements.qld.gov.au/statements/95531.

17 Crime and Corruption Commission, *Operation Impala: Report on misuse of confidential information in the Queensland public sector, February 2020*, https://www.ccc.qld.gov.au/sites/default/files/Docs/Public-Hearings/Impala/Operation-Impala-report-on-misuse-of-confidential-information-in-the-Queensland-public-sector-v2.pdf.

The Crime and Corruption Commission identified 'data breaches' as one of nine broad topics to assist agencies to protect confidential information.[18] It recommended:

> *That a mandatory data breach notification scheme be implemented in Queensland and that the OIC be responsible for developing the scheme, and receiving and managing the notifications. (Recommendation 12)*[19]

It said that one advantage of such a scheme was:

> *The requirement to notify individuals of eligible data breaches was reported as incentivising entities to ensure reasonable steps are in place to adequately secure personal information.*[20]

The Crime and Corruption Commission outlined a practical approach to manage the risks of a data breach:

> *Agencies should have a **response plan** in the event of a data breach. Procedures and a clear articulation of lines of authority should be included in a response plan to assist with containment and management of the breach. It is important to ensure staff, including contractors, are aware of and understand the response plan and imperative of reporting breaches—the OAIC notes this as being essential for the effectiveness of the plan.*[21] (emphasis added)

OAIC has a guide to managing reportable data breaches – *Data breach preparation and response: A guide to managing data breaches in accordance with the Privacy Act 1988* (Cth).

The guide explains that a data breach response plan should outline the entity's strategy for containing, assessing and managing the incident from start to finish.

18 Crime and Corruption Commission, *Operation Impala: Report on misuse of confidential information in the Queensland public sector, February 2020,* page 139, https://www.ccc.qld.gov.au/sites/default/files/Docs/Public-Hearings/Impala/Operation-Impala-report-on-misuse-of-confidential-information-in-the-Queensland-public-sector-v2.pdf.

19 Crime and Corruption Commission, *Operation Impala: Report on misuse of confidential information in the Queensland public sector, February 2020,* page 18, https://www.ccc.qld.gov.au/sites/default/files/Docs/Public-Hearings/Impala/Operation-Impala-report-on-misuse-of-confidential-information-in-the-Queensland-public-sector-v2.pdf.

20 Crime and Corruption Commission, *Operation Impala: Report on misuse of confidential information in the Queensland public sector, February 2020,* page 114, https://www.ccc.qld.gov.au/sites/default/files/Docs/Public-Hearings/Impala/Operation-Impala-report-on-misuse-of-confidential-information-in-the-Queensland-public-sector-v2.pdf.

21 Crime and Corruption Commission, *Operation Impala: Report on misuse of confidential information in the Queensland public sector, February 2020,* page 143, https://www.ccc.qld.gov.au/sites/default/files/Docs/Public-Hearings/Impala/Operation-Impala-report-on-misuse-of-confidential-information-in-the-Queensland-public-sector-v2.pdf.

OAIC states:

> *All entities should have a data breach response plan. A data breach response plan enables an entity to respond quickly to a data breach. By responding quickly, an entity can substantially decrease the impact of a breach on affected individuals, reduce the costs associated with dealing with a breach, and reduce the potential reputational damage that can result.* [22]

A data breach response plan:

- helps agencies limit the likelihood of affected individuals suffering harm
- supports agencies experiencing a breach to lessen their financial or reputational damage
- supports and builds public confidence in agencies' ability to respond to data breaches
- helps agencies meet their legislative commitments to protect and safeguard personal information and privacy.[23]

Since 2018-19, our office (the Office of the Information Commissioner - OIC) has been encouraging agencies to voluntarily report privacy breaches to OIC and affected parties as good practice. We received the first voluntary report of a privacy breach in 2020-21.

This survey anticipates the introduction of a mandatory data breach notification scheme in Queensland. It serves two purposes:

- prompt government agencies to consider and assess their data breach response plan and its contents
- obtain baseline data on agencies' readiness for a MDBN scheme where they will likely have to report eligible data breaches to OIC.

22 Office of the Australian Information Commissioner, *Data breach preparation and response: A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth) – July 2019*, page 12, https://www.oaic.gov.au/__data/assets/pdf_file/0017/1691/data-breach-preparation-and-response.pdf.

23 Adapted from: Office of the Australian Information Commissioner, *Data breach preparation and response: A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth) – July 2019*, https://www.oaic.gov.au/__data/assets/pdf_file/0017/1691/data-breach-preparation-and-response.pdf.

2.3 Mandatory Data Breach Notification schemes in other jurisdictions

Schemes that require mandatory notification to a Privacy Commissioner or regulatory body focus on data breaches involving personal information.

Australia

Australia has a MDBN scheme at the federal level, operated by the OAIC. The *Privacy Amendments (Notifiable Data Breaches) Act 2017* (Cth) amended the *Privacy Act 1988* (Cth) to introduce the mandatory notifiable data breaches (NDB) scheme in 2018.

Under this scheme, federal government agencies and organisations with an annual turnover more than $3 million must report eligible data breaches to OAIC.[24] State government bodies also may have reporting obligations, as outlined in Figure 3.

Figure 3 – Reporting obligations to the OAIC

State government entities' obligations under the NDB scheme
Entities that have obligations under the *Privacy Act 1988* (Cth), or are a credit reporting body, credit provider or Tax File Number (TFN) recipient, may be obliged under the NDB scheme to report the breach to the Office of the Australian Information Commissioner. This may include state government entities that are in possession or control of a record that contains TFN information.

Source: The Office of the Information Commissioner's guideline – Privacy breach management and notification

Not every data breach is eligible to be reported. It must meet certain criteria. OAIC advises:

> *An **eligible** data breach occurs when:*
>
> - *there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an organisation or agency holds*
> - *this is likely to result in serious harm to one or more individuals, and*
> - *the organisation or agency hasn't been able to prevent the likely risk of serious harm with remedial action.* [25]

24 Australian Government agencies (and the Norfolk Island administration) and organisations with an annual turnover more than $3 million have responsibilities under the *Privacy Act 1988* (Cth), subject to some exceptions.

25 Office of the Australian Information Commissioner, *Data breach preparation and response: A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth) – July 2019*, page 9, https://www.oaic.gov.au/__data/assets/pdf_file/0017/1691/data-breach-preparation-and-response.pdf.

The NDB scheme commenced on 22 February 2018.[26] This had an immediate effect. OAIC reported that the number of data breach notifications jumped from 8 notifications in February 2018 to 55 notifications in March 2018.[27]

OAIC provides guidance to agencies and assistance to individuals. It also has the power to intervene to ensure organisations and government agencies meet their legislative obligations. OAIC can enforce compliance with the legislation, and take other regulatory action, for example seek a civil penalty order.[28]

For the period July to December 2022, OAIC received 497 notifications, an average of 83 notifications per month. Most reported data breaches in this period were caused by a malicious or criminal attack (350 breaches, 70%).

A quarter came from human error (123 breaches). The top cause of human error was emailing personal information to the wrong recipient (42%).

New South Wales

New South Wales has amended its legislation to bring in a MDBN scheme. The scheme will take effect from 28 November 2023.[29]

Under the amended legislation, public sector agencies bound by the *Privacy and Personal Information Protection Act 1998* (NSW) must notify the Privacy Commissioner and affected individuals of data breaches involving personal or health information likely to result in serious harm. They must also prepare and publish a data breach policy.[30] Public sector agencies include the state public service, local government authorities, statutory bodies and other specified agencies.[31]

The Act previously required agencies to **prepare** and implement a privacy management plan.[32] This has been updated so that when the amendments take effect, each public sector agency must '***have*** *and implement a privacy management plan*' (emphasis added). There is no requirement to publish the plan.

26 The *Privacy Amendments (Notifiable Data Breaches) Act 2017* (Cth) amended the *Privacy Act 1988* (Cth).
27 Office of the Australian Information Commissioner, *Notifiable data breaches publications,* https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications.
28 On 9 March 2020, OAIC lodged proceedings against Facebook Inc alleging serious and/or repeated interferences with privacy in contravention of Australian privacy law. On 7 March 2023, the High Court made a decision which meant the matter went back to the Federal Court to proceed. OAIC is continuing its action and seeking civil penalties against Facebook Inc.
29 The *Privacy and Personal Information Protection Amendment Act 2022* (NSW), section 2, states the Act commences on the first anniversary of the date of assent. Assent was on 28 November 2022, so the Act is in effect from 28 November 2023.
30 The *Privacy and Personal Information Protection Amendment Act 2022* (NSW) passed Parliament on 16 November 2022 in New South Wales, amending the *Privacy and Personal Information Protection Act 1998* (NSW). The requirement to publish data breach policy is in section 59ZD of the amending Act.
31 *Privacy and Personal Information Protection Act 1998* (NSW), section 3 – Definitions. Note the government has also amended the Fines Act 1996 (NSW) so that all New South Wales public sector agencies are regulated by the same mandatory notification scheme.
32 *Privacy and Personal Information Protection Act 1998* (NSW), section 33.

The privacy management plan and data breach policy may overlap. If so, publishing the policy ensures each public sector agency is transparent and accountable about its processes for responding to data breaches. Non-publication of the plan allows agencies to document plans for prevention or recovery without giving malicious actors the means to circumvent these strategies.

New Zealand

New Zealand also has a scheme for notifying the Privacy Commissioner about privacy breaches under the *Privacy Act 2020*. The Privacy Commissioner uses an interactive online portal to support agencies to identify and report privacy breaches.[33]

2.4 Conclusions

Queensland government agencies should be alert to the introduction of a mandatory data breach notification scheme.

33 Privacy Commissioner, New Zealand, *Privacy breaches*, https://www.privacy.org.nz/responsibilities/privacy-breaches/.

3 Government agency readiness for mandatory data breach reporting

3.1 Introduction

Government agencies have a responsibility to safeguard the handling of personal information under the the Act. In May 2023 we asked them to complete a survey to discover their level of readiness for the introduction of a MDBN scheme.

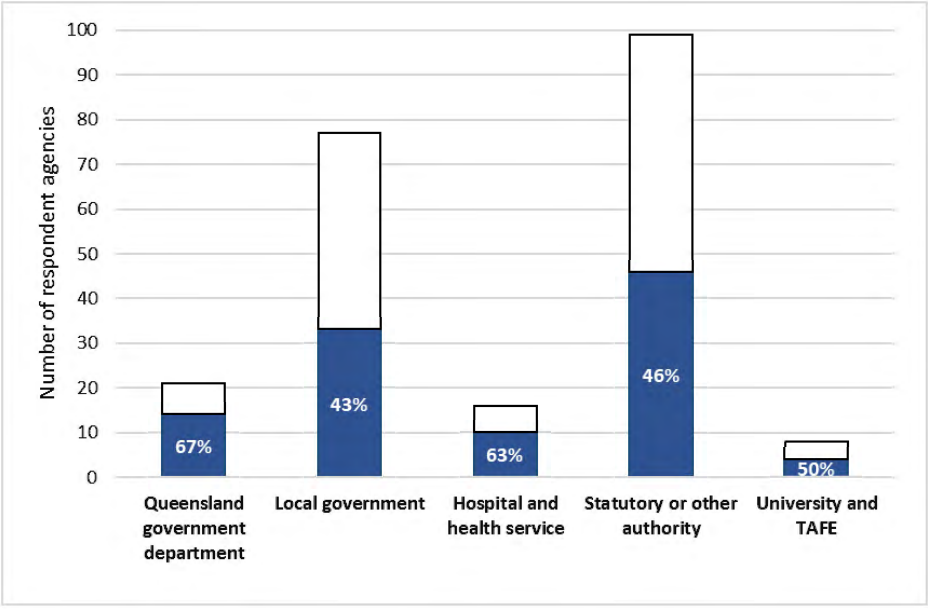
Government agencies include Queensland Government departments, statutory authorities, local governments, hospital and health services, government-owned corporations and universities and TAFE.

The survey asked a series of questions about agencies' data breach response plans. It is based on the OAIC's Data breach preparation and response - A guide to managing data breaches in accordance with the *Privacy Act 1988* (Cth).

Agencies self-reported about whether or not they have a data breach response plan and the elements of their plans. We have not independently verified their responses.[34]

We sent the survey to 221 government agencies in our jurisdiction and received 107 responses across all sectors. Around half or more agencies in each sector responded:

Figure 4 – Survey respondents by sector



Source: Office of the Information Commissioner

34 An audit which does not independently verify facts and findings provides limited assurance.

During the survey and results analysis, we identified three points for consideration about how the MDBN scheme might operate:

- should smaller agencies be able to rely on shared services or larger host agencies to respond to a data breach?
- does the relationship between privacy breaches and data breaches need further clarification?
- are there opportunities to streamline reporting responsibilities in relation to cyber incident reports and reports on privacy or data breaches?

When the Queensland MDBN scheme is implemented, the Queensland government may clarify these points, for example in specific sections in an Act or regulation.

Reliance on shared services or larger host agencies

Six agencies said they did not respond to the survey because they are small agencies that rely on a shared service provider or a larger host agency for policies, procedures and plans.

All agencies, regardless of their size, are responsible for managing their risks, including their data breach and privacy risks. They are also responsible for meeting their legislative obligations.

A shared services provider or a larger agency may assist a smaller agency in meeting their obligations. For example, they could share a policy, template plan or other tools with the smaller agency. The smaller agency should assess the policy or plan and determine whether it meets their needs before tailoring it or adopting it as appropriate.

The relationship between privacy breaches and data breaches

During the survey, a few agencies asked whether privacy breaches and data breaches are the same thing or interchangeable terms.

The *Information Privacy Act 2009* (the Act) does not define the terms ‘privacy breach’ or ‘data breach’. While they relate to each other, they also differ slightly. We discuss them in Chapter 1. For this report, we use these terms according to their ordinary meaning.

MDBN schemes in other jurisdictions do not require agencies to report all data breaches or privacy breaches. To be reportable, breaches must meet a set of criteria. Chapter 2 outlines the criteria set out in other jurisdictions’ MDBN schemes.

The relationship between cyber reports and reports on data breaches

While data breaches are often linked to cyber security incidents, it may not always be the case. For example, an agency may lose data or information if a physical device or document is misplaced or stolen.

Queensland government agencies currently have reporting obligations about cyber security incidents.[35] These might overlap with any future data breach reporting obligations under the Queensland MDBN scheme. We expect the reporting obligations will become clearer with the establishment of the MDBN scheme.

3.2 Findings

The first step for agencies to be ready for the introduction of a MDBN scheme is to have a plan for dealing with data breaches. Currently, there is no legislated requirement for agencies to have a data breach response plan.

However, regardless of mandatory requirements, it is good practice and sound risk management to prevent data breaches and plan an effective response for when the breaches occur. This is also consistent with Queensland Government Enterprise Architecture requirements.[36]

A documented plan

The OAIC guide states:

> *Your data breach response plan should be in writing to ensure that your staff clearly understand what needs to happen in the event of a data breach. It is also important for staff to be aware of where they can access the data breach response plan on short notice.*[37]

We asked:

> *Does the agency have a documented data breach response plan?*

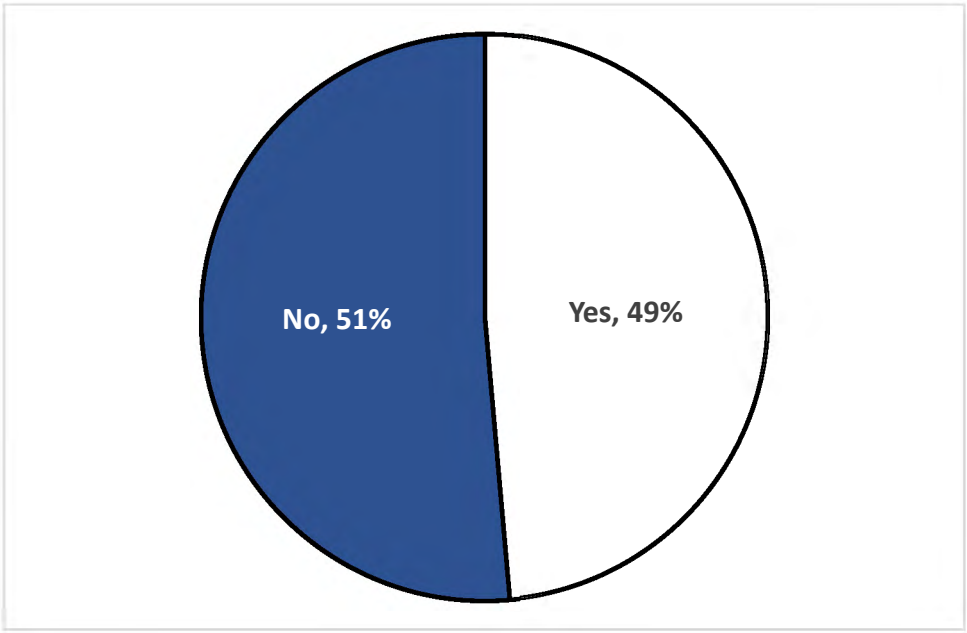
Out of 107 survey respondents, 52 (49%) said yes, as depicted in Figure 5. Of these, 9 plans are in draft and not yet formally adopted.

35 For example, under the Information security incident reporting standard in the Queensland Government Enterprise Architecture, departments must report all cyber security incidents quarterly to the Queensland Government Information Security Virtual Response Team and must report medium impact or breaches affecting multiple systems or departments immediately.

36 Queensland Government Enterprise Architecture, Incident management guideline, https://www.forgov.qld.gov.au/information-and-communication-technology/qgea-policies-standards-and-guidelines/incident-management-guideline.

37 Office of the Australian Information Commissioner, *Data breach preparation and response: A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth) – July 2019*, page 12, https://www.oaic.gov.au/__data/assets/pdf_file/0017/1691/data-breach-preparation-and-response.pdf

Figure 5 – Documented data breach response plan



Source: Office of the Information Commissioner

It is important to note that not having a documented plan does not mean agencies are not managing the risk of data breaches or privacy breaches. A documented response plan is only one element of a broader framework that includes internal controls and strategies to prevent and detect breaches.

Responding agencies may have plans and procedures named differently but covering some or all the elements of a data breach response plan.

For clarity, the rest of this chapter discusses the results for the **52 agencies** who reported having a documented data breach response plan.

An effective plan

For a plan to be effective, agencies need to maintain and test it regularly. They also need to make sure their staff know about the plan and what actions they are required to take.

27 agencies said they have tested their plan: 10 did so using a cyber security exercise, and 12 while responding to an actual privacy or data breach.

Most agencies told their staff about the plan (43 out of 52 agencies), generally through training (14 agencies) or the agency's intranet (18 agencies).

Figure 6 – Methods agencies used to tell staff about their plan

Source: Office of the Information Commissioner

What is in the plan

The OAIC guide says:

> *The more comprehensive your data breach response plan is, the better prepared your entity will be to effectively reduce the risks and potential damage that can result.* [38]

It explains what elements a data breach response plan should cover and provides a checklist about the information to be included in a plan.

Generally, agencies reported their data breach response plan includes key elements but there are gaps.

Explanation and examples

A response plan should explain what constitutes a data breach and provide practical examples tailored to the organisational context. The examples should cover different types of data breaches and varying degrees of seriousness the agency is likely to face.

This helps staff understand what is a data breach, recognise it should one occur and react appropriately.

Figure 7 – Definition and examples

	In plan	Not in plan
Definition of a data breach	50	2
Examples of a data breach	37	15

Source: Office of the Information Commissioner

38 Office of the Australian Information Commissioner, *Data breach preparation and response: A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth) – July 2019*, page 13, https://www.oaic.gov.au/__data/assets/pdf_file/0017/1691/data-breach-preparation-and-response.pdf

We asked agencies:

> *Does the plan outline possible consequences of a data breach?*

Out of 44 agencies who responded that their plans include possible consequences of a data breach, 36 list the risk of serious harm to affected individuals.

The OAIC guide provides the following examples of harm:

- *financial fraud, including unauthorised credit card transactions or credit fraud*
- *identity theft causing financial loss or emotional and psychological harm*
- *family violence*
- *physical harm or intimidation*.[39]

The risk of serious harm to affected individuals is one of the factors to consider when deciding whether to escalate a data breach to a response team. Other factors include the number of people affected by the breach or suspected breach and whether the data breach or suspected breach may indicate a systemic problem.

Roles and responsibilities

A response plan should clearly outline the responsibilities of staff who suspect or detect a data breach. Depending on the circumstances, a line manager could handle a data breach or the breach may need to be escalated to a response team within the agency.

A response team is responsible for taking actions that can reduce the potential impact of a data breach. Who is in the response team depends on the nature of the breach and the agency.

All 52 responding agencies said their plans include information about roles and responsibilities and who to inform if staff suspect a data breach. And 23 responding agencies said their plans explain when a line manager is authorised to handle a breach.

Most agencies (42) agencies said they had established a response team. But only 29 agencies describe the role of the response team members in their plans and 18 agencies provide current contact details for the members of the response team.

39 Office of the Australian Information Commissioner, *Data breach preparation and response: A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth) – July 2019*, page 8, https://www.oaic.gov.au/__data/assets/pdf_file/0017/1691/data-breach-preparation-and-response.pdf

Figure 8 – Response team

The plan outlines	Yes	No
Who is a member of the response team:	34	8
• the authority or delegations of each member of the response team	19	15
• the current contact details for the response team members	18	16
• when to include outside experts in the response team	23	11

Source: Office of the Information Commissioner

Of the 42 agencies who reported having a response team, 35 said their plans outline when to escalate a data breach.

Response strategies

A response plan should cover potential strategies for containing and remediating data breaches. It should also explain how the strategies will apply to various types of data breaches and varying risk profiles. This helps staff take appropriate action quickly.

The majority (87%) of responding agencies said their plans include potential response strategies, but the plans of only 20 agencies explain how the strategies apply to various types of data breaches and risk profiles.

We asked agencies

> *Does the plan outline the agency's policy about assessing a data breach?*

Most agencies (44) said yes and listed the factors to consider when assessing a data breach, as shown in Figure 9.

Figure 9 – Factors to consider when assessing a data breach

	In plan	Not in plan
Type or types of personal information involved in the breach	43	1
Types of individuals whose personal information is involved in the data breach (for example individuals known to be vulnerable)	36	8
Cause of the breach	36	8
Extent of the breach – systems, volume of information	37	7
Extent of the breach – potential number of affected individuals	38	6
Nature of the harm to affected individuals	40	4
Likelihood of the harm to affected individuals	41	3
Effectiveness of possible remediation actions to remove the harm	28	16
Length of time the information has been accessible	25	19

Source: Office of the Information Commissioner

When agencies evaluate how a data breach occurred and how well they responded, they can improve their data management practices and strengthen the protection controls. Most agencies (37) reported having a policy about reviewing their response to a data breach.

Communication

A data breach response plan should include a clear communication strategy that allows prompt notification of the relevant stakeholders. These can include external agencies such as law enforcement and cyber security agencies, regulators, insurers; and, if the data breach involves personal information, the affected individuals.

The communication strategy should also identify who to notify within the agency, for example executive management, the legal unit and/or the privacy officer.

The timing and method of communication may vary as the response to, and assessment of, the data breach evolves.

While 30 agencies reported that their plans include a communication strategy, a greater number of agencies have guidance about communication in their plans, for example that external stakeholders may need to be notified.

Figure 10 – Notification

	In plan	Not in plan
Agency's executive	43	9
External notifications eg to NDB or insurers	36	16
Notification of affected individuals	37	15
OIC identified as a stakeholder to contact	42	10

Source: Office of the Information Commissioner

Although 37 agencies reported that their response plan considers whether to notify individuals, there is less detail about how to notify them (21 agencies) and when (26 agencies).

3.3 Conclusions

About half the responding agencies said they have a documented data breach response plan. It does not mean agencies are not managing the risk of data breaches or meeting their obligations to protect personal information. A documented response plan is only one element of a broader framework that includes internal controls and strategies to prevent and detect breaches.

Responding agencies may have plans and procedures named differently but covering some or all the elements of a data breach response plan.

The answers of the 52 responding agencies with a documented data breach response plan indicate some plans are more comprehensive than others. For example, all 52 agencies said their plans outline roles and responsibilities and who to inform if staff suspect a data breach, but only 37 agencies give examples of data breaches.

Similarly, 45 agencies said their plans include potential response strategies, but only 20 agencies explain how the strategies apply to various types of data breaches and risk profiles.

Most agencies (42) reported they had established a response team. This can help responding to data breaches quickly and more effectively.

The same number of agencies (42) identify OIC as a stakeholder to contact in the event of a data breach.

4 Appendix – Survey methodology and resources

The Office of the Information Commissioner (OIC) conducted this survey under section 135 of the *Information Privacy Act 2009* (Qld). It is part of our role to conduct reviews into personal information handling practices of government agencies, including technologies, programs, policies and procedures, to identify privacy related issues of a systemic nature generally. The survey ran from 26 April to 12 May 2023.[40]

The survey introduction and questions are listed below. Most questions required a 'yes' or 'no' response. Some questions had options or allowed for open text. We coded some open text responses using standardised codes to facilitate analysis.

Survey introduction – Data breach response plan

The final report of the Coaldrake review (https://www.coaldrakereview.qld.gov.au) recommended *'a mandatory data breach notification (MDBN) scheme be established in Queensland, forthwith.'*

This echoes the recommendation from the CCC's Operation Impala in 2020 that '*a mandatory data breach notification scheme be implemented in Queensland and the OIC be responsible for developing the scheme, and receiving and managing the notifications*.'

On 28 June 2022, the Premier indicated that the Queensland Government will accept all the recommendations from the Coaldrake review and will implement them.

The Office of the Information Commissioner (OIC) is conducting this survey under section 135 of the *Information Privacy Act 2009* (Qld). It asks a series of questions about **your agency's data breach response plan**. Most questions are binary yes/no questions.

This survey will establish baseline data on government agencies' level of preparedness to respond to a data breach. Government agencies include Queensland Government departments, statutory authorities, local governments, hospital and health services, government-owned corporations and universities and TAFE.

We will collate the results of this survey and present them in an aggregated format in a report to Parliament.

* Required

Y – yes

N – no

40 The Queensland Government redistributed the public business of the State in Administrative Arrangements Order (No. 1) 2023, made by Governor in Council on 18 May 2023, after the survey was conducted. If we re-ran the survey, some agency responses might now be different, depending on their new responsibilities.

All Possible Survey Questions (Note – some questions only presented as a follow-on from a preceding response)				
Agency details				
1	Name of the agency *			
2	Type of agency *			
	◯	Queensland Government Department		
	◯	Local Government		
	◯	Hospital and Health Service		
	◯	Statutory Authority		
	◯	University and TAFE		
	◯	Government Owned Corporation		
	◯	Other		
Contact details				
3	Name of the person completing this survey on behalf of the agency *			
4	Position *			
5	Business email address *			
Data breach response plan			Y	N
6	Does the agency have a **documented** data breach response plan? *			
7	When was the plan approved? *			
8	Has the agency reviewed the plan since it was approved? *			
9	Date of the most recent review * _____			
10	Date of the next scheduled review _____			
11	Has the agency tested the plan? *			
12	Date of the most recent test * _____			
13	What did the test involve? * _____			

14	Date of the next scheduled test _____		
15	Has the agency made its staff aware of the data breach response plan? *		
16	How has the agency made its staff aware of the plan? *		
17	Has the agency published its data breach response plan, or a version of it, on its website? *		
Definitions		Y	N
18	Does the plan clearly explain what is a data breach? (*A data breach occurs when personal information that an entity holds is subject to unauthorised access or disclosure, or is lost* - page 7 Data breach preparation and response, OAIC) *		
19	Does the plan give examples of data breaches? *		
20	How many examples of data breaches are in the plan? * (the value must be a number)		
21	Does the plan outline possible consequences of a data breach? *		
22	Does the plan identify risk of serious harm to affected individuals as a possible consequence of a data breach? *		
Role and responsibilities		Y	N
23	Does the plan outline roles and responsibilities in case of a data breach? *		
24	Does the plan explicitly state who staff should inform if they suspect a data breach? *		
25	Does the plan outline the circumstances in which a line manager can handle a data breach? *		
26	Has the agency established a data breach response team? *		
27	Does the plan explain when a data breach must be escalated to the response team? *		
28	Does the plan identify who is responsible for deciding whether to escalate to the response team? *		

29	Does the plan specify the factors to consider when deciding whether to escalate to the response team? *			
30	According to the plan, what factors should be considered when deciding to escalate to the response team? (select all that apply) *			
	◯	the number of people affected by the breach or suspected breach		
	◯	the risk of serious harm to affected individuals now or in the future		
	◯	whether the data breach or suspected data breach may indicate a systemic problem in the agency		
	◯	the value of the data to the agency		
	◯	the reputational risk to the agency		
	◯	other		
Response team			Y	N
31	Does the plan clearly identify each member of the response team? *			
32	Does the plan describe the roles and responsibilities of each member of the response team? *			
33	Does the response team include a senior member of staff with overall accountability and expertise about privacy? *			
34	Does the plan describe the authority or delegations of each member of the response team? *			
35	Does the plan include **current** contact details for each member of the response team? *			
36	Does the plan outline the circumstances (for instance the nature of the breach) in which the agency may need to include external experts in its response team, for example legal advice, data forensics, or media management? *			

Strategy for containing, assessing and managing data breaches			Y	N
37	Does the plan include the actions the agency will take in the event of a data breach or a suspected data breach? *			
38	Does the plan include potential strategies for containing and remediating data breaches? *			
39	Does the plan explain how the containment and remediation strategies will apply to various types of data breaches and varying risk profiles? *			
40	Does the plan include legislative or contractual requirements applicable to the agency (such as the requirements of the NDB scheme or an insurance contract)? *			
Communication strategy			Y	N
41	Does the plan include a clear communication strategy? *			
42	Does the communication strategy allow for the prompt notification of ? *			
	◯	affected individuals		
	◯	external stakeholders (for example law enforcement and cyber security agencies at state and federal levels, regulators such as OIC and OAIC, insurance, etc)		
	◯	agency executives		
	◯	other		
43	Does the plan specify who is responsible for implementing the communication strategy? *			
44	Does the plan explain how to determine whether to notify affected individuals? *			
45	According to the plan, what factors should be considered when determining whether to notify affected individuals? (select all that apply) *			
	◯	the type or types of personal information involved in the data breach		
	◯	the circumstances of the data breach, including its cause and extent		

	◯	the nature of the harm to affected individuals, and if this harm can be removed through remedial action.		
	◯	other		
46		Does the plan identify who is responsible for determining whether to notify affected individuals?*		
47		Does the plan outline **how** affected individuals will be contacted and managed? *		
48		Does the plan outline **when** affected individuals will be contacted? *		
49		Does the plan include criteria for determining which external stakeholders should be contacted (for example, law enforcement and cyber security agencies, regulators such as the OAIC, and the media)? *		
50		Is OIC mentioned in the list of external stakeholders to be contacted under the current voluntary data breach notification scheme? *		
51		Does the plan identify who is responsible for liaising with external stakeholders? *		
52		Does the plan explain how to determine whether to notify the agency's executive? *		
53		Does the plan identify who is responsible for determining whether to notify the agency's executive? *		
Documentation and review			Y	N
54		Does the plan outline the agency's policy about recording and documenting data breaches? *		
55		Does the policy include recording data breaches that are not escalated to the response team? *		
56		Does the plan or the policy identify who is responsible for documenting and recording data breaches? *		
57		Does the plan outline the agency's policy about assessing a data breach? *		
58		According to the plan or the policy, what factors should be considered when assessing a data breach? (select all that apply) *		

	◯	the type(s) of personal information involved in the breach		
	◯	the individuals whose personal information is involved in the data breach (for example individuals known to be vulnerable)		
	◯	the cause of the breach		
	◯	the extent of the breach - systems, volume of information		
	◯	the extent of the breach - potential number of affected individuals		
	◯	the nature of the harm to affected individuals		
	◯	the likelihood of harm to affected individuals		
	◯	the effectiveness of possible remediation actions to remove the harm		
	◯	the length of time the information has been accessible		
	◯	other		
59	Does the plan outline the agency's policy about documenting and recording the assessment of a data breach? *			
60	Does the plan or the policy identify who is responsible for documenting and recording the assessment? *			
61	Does the plan outline the agency's policy about reviewing the response to a data breach? *			
62	Does the plan or the policy identify who is responsible for reviewing the agency's response to a data breach? *			
63	Does the review include amending the agency's data breach response plan where applicable, as a result of reviewing the response to a breach? *			

The survey listed possible resources that may help agencies develop or enhance a data breach response plan.

Resources
https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/privacy-compliance/privacy-breach-management-and-notification
https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/responding-to-a-privacy-breach
https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/preventing-preparing-for-and-responding-to-data-breaches/data-breach-preparation-and-response
https://www.forgov.qld.gov.au/information-and-communication-technology/cyber-security