Breach Management

Overview

There are key components that an organisation needs to have in place to manage privacy breaches successfully – we call this a breach management system. A tested and integrated incident response plan is crucial because it helps organisations respond appropriately when a serious breach occurs or can prevent a breach from becoming serious because of an unprepared response.

A robust breach management system is also an important source of data to inform your privacy work programme. The implementation of a breach management system requires communication across the business, which will raise the profile of privacy within your organisation.

In this pou we are focusing on three key aspects of breach management:

- Responding to a breach or privacy incident, including notifying OPC and affected individuals.
- Reporting on incidents internally and managing them.
- Reflecting on the incident and response.

While this pou is primarily concerned with notifiable breaches, the information will be useful for thinking about responding, reporting, and reflecting on interferences with privacy and other breaches (such as breaches of the privacy principles that don't cause harm).

Who is this for?

Your privacy function and anyone within the organisation who has a responsibility for privacy incident management. In smaller organisations, this may be an individual privacy officer. In larger organisations, there may be some specific privacy roles that focus on responding, reporting and reflecting on privacy breaches.

Key objectives of the Breach Management pou

What would we expect to see?

- The organisation has a fully tested incident response plan. This means the plan is practiced in a mock situation.
- The timeframe for deciding to report a breach, and reporting a breach, complies with OPC expectations.
- Incident log records both actual breaches and near misses.
- Staff know how to identify a possible breach and escalate to the appropriate person or team.

Respond

Identify

What is a notifiable privacy breach?

A notifiable privacy breach occurs when personal information held by an organisation is:

- accessed, disclosed, altered, lost, or destroyed accidentally or without authorisation, or
- cannot be accessed by the organisation on a temporary or permanent basis. For example, it's encrypted by ransomware; **and**

has either caused, or is likely to cause, serious harm to someone whose information was affected by the breach.

Common privacy breaches include:

- Personal information e.g. postal address, email address, or mobile phone number, being sent to the wrong recipient.
- Personal information being accidentally sent to others. For example, sending on an email chain, failing to use 'blind copy' (bcc) on an email to multiple recipients, or attaching the wrong document to an email.
- Employees accessing personal information without a proper purpose (known as employee browsing).
- Disclosing personal information without a lawful basis.
- Computers, removable storage devices, or documents containing personal information being lost or stolen.
- Hardware being thrown away, recycled, or returned to leasing companies without personal information being deleted first.
- Personal information being accessed by an unauthorised third party, for example, a hacker gaining login credentials via a phishing email.
- Organisations losing the ability to access personal information on its systems, for example, a security patch that fails and allows the system to be corrupted, or a ransomware attack.
- Breaches of third-party providers who store or process information on behalf of your organisation.

What is serious harm?

The unauthorised sharing, exposure, use or loss of access to personal information may cause serious harm to impacted individuals or groups. Some types of information are inherently more sensitive than others, and therefore more likely to cause serious harm. You should also consider what you know about the people who have been impacted by the breach, as some people are particularly vulnerable or at a greater risk of harm. For example, victims of family violence.

Types of serious harm include:

- Physical harm or intimidation.
- Financial fraud, including unauthorised credit card transactions or credit fraud.
- Identity theft.
- Psychological or emotional harm.

- Employment harm such as the loss of a job opportunity or work assignment.
- Blackmail e.g. threat of publishing sensitive information.
- Threats to national security.
- Kidnapping.
- Theft of significant amounts of money.
- A risk that an individual's life could be in danger.

If you suspect a privacy breach may result in imminent harm to an individual, you should notify the NZ Police immediately before reporting the breach to OPC through Notify Us.

Contain

Once you discover a privacy breach has occurred, you should act immediately to contain it.

Steps to help contain a breach may include:

- Taking steps to reduce the impact of the breach. For example, recalling an email, or requesting deletion by the recipient.
- Assembling your response team. This may include people from within the organisation as well as external parties that have the expertise to deal with the situation (such as IT experts or risk advisors).
- Appointing someone within the organisation to lead and conduct an initial investigation into what has happened or bring expert advisors in to assist. This initial investigation can focus on identifying immediate mitigation steps required to contain the breach. A more detailed review on how it occurred, and how to prevent it reoccurring, can be carried out later.
- Diagnosing what went wrong and disabling any systems that may be compromised until they have been secured.
- Remotely wiping information from devices that have been lost or stolen if you can do so.
- Where personal information has been received or circulated in error, considering whether it's possible and appropriate for your IT team or computer admin to purge these records.
- Trying to retrieve lost information, e.g. if you have sent a letter to the wrong person, see if you can get the recipient to give it back unopened.
- Cancelling or changing computer access codes and fixing any weaknesses in the organisation's physical or electronic security.
- Considering who outside the organisation needs to be told about the breach, such as CERT NZ or NetSafe (for more information on notifying OPC, read "Notifying the Office of the Privacy Commissioner" below). Assess whether your insurer, internal auditors, risk managers and legal advisors need to be informed. If the breach involves theft or other criminal activity, inform the Police.
- In serious breaches, especially those involving criminal activity, you could consider applying to the High Court for an injunction to help contain the breach and prevent further harm from arising.

Assess

Assessing a privacy breach as quickly as possible can help an organisation understand the steps needed to appropriately respond alongside any action taken to contain the breach.

Knowing the scope of the personal information involved and the nature of the individuals impacted will help you determine whether serious harm has occurred or is likely to occur and what your notification obligations are.

For example, a leaked list of clients of a specialist mental health service provider is likely to be more sensitive and therefore more likely to cause serious harm to the individuals affected than a leaked list of subscribers to a newspaper.

The criteria for assessing the likelihood of serious harm are outlined in section 113 of the Privacy Act 2020.

Those criteria are:

Any action taken by the organisation to reduce the risk of harm following the breach

Have you taken steps to contain the breach? How quickly were you able to take them? How effective or successful were these steps?

Do you have an incident response plan? Such a plan outlines the procedures that your organisation will take following a breach. See the Reflect section in this document for further guidance on what should be included in an incident response plan.

Try to identify the size and scope of the breach, including the number and nature of the likely recipients as well as the number of affected people. Identify the risk of the information being circulated further and respond accordingly.

Whether the personal information is sensitive in nature

Certain types of information are more likely to lead to harm than others. For example, financial or identification documents can lead to fraud or identity theft. Other types of sensitive information include information relating to someone's biometrics, health, genetic or ethnic background, political or religious beliefs, sex life or sexual orientation, or whether someone has committed any crimes.

The personal information of children and young people is also more likely to be considered sensitive.

Context matters. Personal information that might not normally be considered sensitive, such as email addresses, may be considered sensitive in specific circumstances. For example, where a person with a protection order in place has their home address shared.

The opposite can also be true; some information may be inherently sensitive but may not be sensitive in the specific circumstances. For example, if the information has gone to someone who already knows it or it's already publicly available.

The person or body that has obtained or may obtain personal information because of the breach (if known)

Was the receiver a trusted, known person or organisation that can be expected to return the information? Were they under any kind of obligation of confidentiality or secrecy, similar to that of a doctor or lawyer?

Or was the information taken by, or given to, an unknown receiver, someone who might pose a particular risk, or to a wide range of people with the potential to misuse the information?

For example, if the breach was caused by a malicious actor who used unlawful means to access the information, this increases the likelihood that they intend to misuse any information they obtain.

Knowing, and even not knowing, who has received the information will shape how you respond.

Whether the breached personal information is protected by a security measure

This factor is about security measures that are designed to protect the breached personal information from being accessed and misused either accidentally or maliciously once it has been breached. It is not about the security of the system that the personal information came from.

If breached personal information is password protected or encrypted, there is a lesser chance of it being accessed and misused than if it is unprotected. Likewise, if the breached personal information is on a lost or stolen laptop that can be remotely wiped, this would reduce the chances of access and misuse.

You should consider whether the security measures that protect information involved in a breach are likely to be effective at preventing access to it in the circumstances.

Any other relevant matters.

Notify

Being open and transparent with people about how personal information is being handled is a fundamental rule of privacy, especially when there has been a breach. Notification can also be a key step in helping people affected by a breach.

If a privacy breach creates a risk of serious harm to people, those affected need to be notified, unless one of the exceptions in the Act applies. Prompt notification can enable people to take steps to protect themselves and regain control of their information.

Notifying the Office of the Privacy Commissioner

You must inform the Privacy Commissioner of serious privacy breaches as soon as you practically can after becoming aware of them. Our expectation is that you will do this within 72 hours of becoming aware that it's a notifiable breach. This timeframe is a guide only and is intended to initiate prompt notification to us.

In some cases, it will be clear from the outset that a breach has occurred and that it is notifiable. In other cases, an organisation may not discover the breach immediately or may need to undertake some enquiries to figure out whether a breach has occurred or is serious (for example, where an audit of an employee's access raises questions about inappropriate access).

OPC's Notify Us tool can help you assess how serious your breach is and whether you will need to notify the Privacy Commissioner. This tool is a guide only, so if you're not sure, please notify. If you do need to notify OPC, you can also do this using Notify Us.

What does 'becoming aware' mean?

Becoming aware of a notifiable breach requires some degree of knowledge or an assessment about the risk of harm from the privacy breach. This will be a straightforward

assessment for some breaches, while others may be more complex or have unique facts or circumstances.

The key thing is once your initial assessment indicates that harm is likely based on what you know at that time (e.g. sensitivity of the information, weakness in security measures, and probable harm to individuals) you should be thinking about prompt notification, even if there are still some unknowns (such as who has obtained or could obtain the information).

Information known by your employees or agents (third-party providers) is treated as being known by the organisation. This means that a privacy breach can be notifiable as soon as any employee or agent identifies that it is notifiable, not just your privacy officer. You need to ensure that your processes support prompt disclosure of privacy incidents to your privacy function and that you promptly act upon that information, including undertaking further investigation and assessment where necessary.

Incremental notification

We understand that not all information will be available at the same time. An organisation can fulfil its notification requirements to our Office and affected individuals on an incremental basis, under section 117(5) of the Privacy Act, so long as the organisation does this as soon as reasonably practicable after finding out that information. However, you should still let us know as much as you can. You can provide any subsequent updates to us at notifyus@privacy.org.nz using the PBN/xxxx number provided.

If your assessment is that notification is not required, you need to regularly review that as your breach response or investigation progresses and the information that you have changes (for example, you may discover that the lost USB key was not encrypted).

Document your decision-making

It's important to keep good records. Your assessment of the breach, decision whether to notify, and the reasons for that decision should be well documented. Recording reasons at the time helps to support good decision-making and promote accountability. It also helps you to explain and justify the decisions if any concerns are raised, or you need to provide additional information to OPC and individuals. You can print a copy of your notification to OPC for your records.

Case study A

A privacy officer at Very Large Tech Company Ltd hears from a cyber-security staff member at the company that they have identified unusual activity on the company servers but are still working out the details. The privacy officer joins the incident response team to support them to work quickly to identify whether the issue is a privacy breach. It becomes clear the next day that personal information has been accessed by a hacker for ransom, but it's not clear exactly what personal information has been accessed, what has happened to it and how many people have been impacted. However, as personal information has been criminally accessed, it's reasonable to conclude that serious harm is likely. Hackers are known to post the data on the dark web and use or sell identity data for fraudulent purposes, even when a ransom is paid by the organisation. This means the privacy officer must notify the Office of the Privacy Commissioner as soon as practicable and within 72 hours, which they do via Notify Us. They continue learning more about the breach, so they update the breach notification to the Commissioner incrementally and notify affected individuals via a public

notice and then individually once they have established whose information was compromised and locate their contact details.

Case study B

A member of the public emails the privacy officer at Very Large Tech Company Ltd to tell them that they have a file of the Company's hard-copy papers which they found on a train. The email doesn't say what is in the file, and it takes a couple days for the individual to respond to the Privacy Officer's calls. During the phone call, the individual says that they got the company's details from a policy document that was on the file but didn't look through the other documents. They also say that they are happy for the Privacy Officer to collect the file, but not for another 5 days as they are away on holiday. At this stage, the Privacy Officer records their view that they don't think that there is a notifiable privacy breach as the individual has proactively notified the Company, has taken steps to secure the file, and says that they have only seen a policy document.

The Privacy Officer collects the file as soon as the individual returns from holiday. On review, they discover that the file contained a document with highly sensitive personal information about another employee at the Company. As the file was unsecured while on the train and could have been accessed by a member of the public prior to the individual securing it, the Privacy Officer revises their decision and decides that there has been a notifiable privacy breach and notifies OPC as soon as practicable and within 72 hours. They also work with the Company's HR department to notify the affected employee.

Once OPC receive a breach notification

After you have notified us of a privacy breach, any action we take will depend on the nature of your breach, the number of people impacted, and the actual or potential harm.

Other actions we may take include:

- Asking for further information from the notifying organisation.
- Providing advice on responding to the incident and any other notification requirements.
- In cases where an organisation is failing to take appropriate steps promptly, we may encourage or require the organisation to protect the privacy interests of the individuals affected.
- Assessing the cause of the incident to determine if there were any areas of non-compliance with Privacy Act requirements.
- We prefer to work with organisations to gain the best outcomes for affected individuals to avoid it happening again.

Notifying individuals affected by the breach

Where there is a notifiable privacy breach, you will also need to notify the people affected unless an exception applies. These exceptions include situations where notifying them would adversely affect that person's health or wellbeing. If law enforcement authorities are involved because the breach involves criminal activity, you may want to check with those authorities before you notify so that their investigation isn't compromised.

If there is no risk of serious harm, you are not required to notify people of a privacy breach, but you may still choose to. You may decide that it's in the best interests of the affected

individuals to be informed. Each incident needs to be considered on a case-by-case basis. Being open and transparent with customers and employees when things go wrong can help build trust in how your organisation manages and protects the personal information it's responsible for.

When notifying people, it's important that you have as much information as possible about what happened and what information of theirs was impacted. Incorrectly notifying the wrong people that their information has been breached may cause them unnecessary stress and harm. If you're notifying people, and you don't have all the details yet, it's important to be open about that. You should let them know what's happening, when, and who they can get support from.

Things to consider:

- Is this a notifiable privacy breach? What is the risk of harm to people whose information has been breached?
    - Is there a risk of identity theft or fraud?
    - Is there a risk of physical harm?
    - Is there a risk of humiliation or loss of dignity, or damage to someone's reputation or relationships? For example, when the breached information includes mental health, medical, or disciplinary records.
- What is the person's ability to avoid or minimise possible harm?
- What are your other legal and contractual obligations?
- Your notification requirements, including considering the impact that notification of a breach may have on vulnerable people. You may then consider if it's better to notify a representative or to inform them with particular care.

Organisations should notify affected individuals directly. However, there are circumstances where it may be appropriate to issue a public notice instead. For example, where many affected individuals cannot be directly contacted.

You are not required to notify the people involved, or give public notice, of a notifiable privacy breach, if you believe that the notification or public notice will:

- Prejudice the security, defence, or international relations of New Zealand.
- Prejudice the maintenance of the law by a public sector organisation.
- Endanger someone's safety.
- Reveal a trade secret.

Who should notify affected individuals?

There may be multiple organisations involved in managing a breach.

You will need to work out who will be responsible for notifying the Office of the Privacy Commissioner and affected individuals, and any ongoing communications. This will require you to step through which organisations are legally required to notify. This will depend on whether your organisation is 'holding' the information that has been compromised.

For example, if a service provider (A) processes information on behalf of another organisation (B) and does not use the information for its own purposes, the breach notification obligation rests with the organisation (B). (B) will want to ensure it has contractual protections in place so that if (A) suffers a breach that impacts (B)'s data, (A) is required to tell (B) immediately and take steps to manage the breach.

However, if (A) uses the information for its own purposes, both (A) and (B) will have notification obligations. While in practice, (A) and (B) could agree in contract that one of them will notify on behalf of the other, they will need to ensure that the contracted party takes appropriate action to fulfil the notification obligations.

Generally, the organisation that has the closest relationship with the affected individuals should be the one to notify them, but the notification should be clear that it is being made on behalf of multiple organisations.

What to say?

Under section 117(2) of the Privacy Act, breach notifications to individuals must include:

- Information about the incident, such as a description of the information that was disclosed and what hasn't been disclosed.
- Whether the organisation has identified who might be in possession of their personal information (the organisation shouldn't include any information that could identify that person or body, unless considered necessary to prevent or lesson a serious threat to the life or health of an individual).
- What the organisation is doing to control or reduce the harm. This could include general information about the potential types of harm that could be caused, given the personal information involved.
- What the organisation is doing to help people and what steps the affected people can take to protect themselves.
- Confirmation that the Commissioner has been notified under section 114.
- That they can make a complaint to the Office of the Privacy Commissioner and information on how to do that.
- Contact information of an individual within the organisation for enquiries and complaints.

Notifying someone else

You don't need to notify a person about, or give public notice of, a notifiable privacy breach involving their personal information if:

- The person is under the age of 16 and you believe that the notification or public notice won't be in their interests, or
- After you first consult that person's health practitioner (where practical), you believe that the notification or public notice will likely prejudice that person's health.

However, in those circumstances, you must:

- First think about whether it would be more appropriate to contact the person's parent, guardian or other representative, and
- Before deciding whether to contact the person's parent or guardian, consider the person's individual circumstances and the circumstances of the privacy breach itself.

Then, you must notify the person's parent, guardian or other representative (rather than notify the person involved or give public notice).

If you are not intending to notify, the Privacy Commissioner is likely to seek further information from you on this decision.

Delaying notification or public notice

You can also delay notifying the people involved, or giving public notice, if you believe that:

- The notification or public notice may have risks for the security of personal information that you hold. For example, if you must patch a security exploit to avoid a further privacy breach. And,
- Those risks outweigh the benefits of informing the affected people at that time.

You can only delay the notification or public notice while those risks continue to outweigh the benefits. This decision should be continuously revisited throughout the process of managing the breach.

Regardless, you must not delay or refuse to tell OPC about a notifiable privacy breach.

How should you notify people?

It is always best to notify affected people directly – by phone, letter, email, or in person. Direct notification is more sincere and personal.

Public notices

Where it is not reasonably practical to notify individuals directly, you may issue a public notification.

Examples of where it's not practical for an organisation to notify people individually of a breach could be when the organisation doesn't know exactly which people were affected by a breach, or when you don't hold accurate contact details for those affected.

Public notices must be published on the organisation's website and must be publicly accessible and free of charge. The notice needs to be in at least one other format that will bring the notice to the attention of the greatest number of affected individuals. Consider your audience and traditional channels, such as radio or television, as well as social media. Under regulation 12 of the Privacy Regulations 2020, the public notice must:

- Describe the notifiable privacy breach, without identifying any affected individual.
- State any steps that an affected individual can take to mitigate or avoid potential loss or harm.
- Confirm that the Privacy Commissioner has been notified of the privacy breach.
- State that an affected individual has the right to make a complaint to the Privacy Commissioner about the privacy breach.
- Include the contact details of a person within the organisation that inquiries about the privacy breach can be sent to.

Notifying third parties

Organisations should consider whether the following groups or organisations should also be informed. Bear in mind any obligations of confidentiality, as well as any contractual or other legal obligations that you may have.

- Police.
- Insurers.
- Professional or other regulatory bodies.
- Credit card companies, financial institutions, or credit reporting agencies.
- Third party contractors or other parties who may be affected.
- The government minister.

- Union or other employee representatives.

Report

Keeping an incident record

Capturing all privacy breaches and near misses in a log will help you manage the breach and identify risks that could make a breach more likely to occur. It also helps you to develop a plan to improve your process and systems.

We do not suggest that you set a target of zero breaches, as it discourages the reporting of breaches and incidents and the important insights that your organisation can gain from them.

Information you can capture in the log:

- Date of the incident and date it was identified.
- Type of incident:
    - unauthorised access
    - unauthorised disclosure
    - email or postal error
    - employee browsing
    - loss/theft of physical documents
    - loss/theft of IT equipment
    - website/IT system error
    - disposal error, and/or
    - cyber-attack.
- Cause of the incident.
- Scale of the incident (e.g., how many individuals were affected).
- Type of personal information that was subject to the incident (e.g., employment information, financial information).
- Intention behind the incident, if known (e.g., accidental, intentional, or malicious).
- Who accessed the personal information (e.g., an employee, or someone external to the organisation).
- Nature of the harm for affected individuals (e.g., emotional harm, financial loss).
- Nature of the harm for your organisation (e.g., reputational risk, financial loss).
- Business unit where the incident originated.
- Response to the incident.

Consider using dropdown menus instead of free text wherever possible. This will help with data analysis, trend analysis, and anomaly detection. Dropdown menus can also minimise the risk of users entering erroneous data.

It's important to keep in mind that an incident log can be a sensitive document in and of itself, due to the type of information that may be captured when describing an incident or privacy breach.

You shouldn't capture any personal information in these logs. Instead, you could use a unique identifier, such as a file number, so that information can be linked back to the actual incident.

For example, if recording incidents of employee browsing, it is crucial to preserve the confidentiality of any investigations or disciplinary processes. You should ensure only the minimum amount of information is captured in the reporting log.

You should have controls in place to manage who has access to the log itself, and then look to facilitate wider access to the information in safe, aggregated ways for reporting purposes.

What about near-misses and non-notifiable privacy breaches?

Fortunately, there are many occasions when somebody realises a privacy breach is about to happen and acts before it's too late. Similarly, sometimes privacy breaches occur but serious harm is not caused.

Many of the most common privacy breaches are easily preventable, and all these circumstances provide an opportunity for organisations to learn and make system changes to avoid a serious breach next time.

Often organisations or individuals will narrowly avoid serious privacy breaches through sheer luck.

For example, you might be about to send an email containing personal information to the wrong person.

You may have drafted an email containing sensitive information to a list of people and cc'd in each email address rather than bcc'd. In each of these instances, a breach could be avoided if, just before clicking 'send', you realise your mistake and take appropriate action to avert a breach.

Other examples of narrowly avoiding serious privacy breaches could be:

Near misses

- When an email or letter containing sensitive personal information is sent to the wrong person, and the mail is returned unopened.
- If a website vulnerability that exposes personal information is discovered by staff before any website users see it.
- If a 'business' CCTV camera has the audio function enabled, but this is discovered and addressed before inadvertently capturing audio of private conversations.

Non-notifiable privacy breach

- If someone sends an email to the wrong recipient, but it contains no sensitive personal information. While a privacy breach has happened, because no serious harm has or is likely to occur, you would not need to notify OPC or the affected individuals.

Prevention is better than cure – near misses provide the perfect opportunity for organisations to examine how they handle customer or client information and improve their privacy game.

You can still notify the Office of the Privacy Commissioner of breaches that aren't likely to cause serious harm. This provides an opportunity for OPC to give you advice and direction on how to reduce the likelihood of it occurring again, or in a way that does cause serious harm.

Reflect

Lessons learned

There are always new lessons learned from every incident. You should plan a debrief meeting with the key people involved after the incident has settled. The meeting will help you to identify any systemic risks, whether any changes are required to systems and processes, and whether there is a need for additional privacy training and awareness for staff.

You should always include a root cause analysis as part of the debrief:

- What happened?
- Why did it happen?
- What can be done to prevent another incident from happening again?

Note that the root cause is the fundamental reason for the incident occurring. For example, the root cause of a cyber-hack could be a low security password or access setting, or an IT security patch not being applied in a timely way. The root cause of human error may be a multi-step operational process that drives staff to create a workaround that increases the likelihood of mistakes.

You should also take the time to consider how the incident was managed overall:

- What worked/didn't work?
- Were there any blockers which impacted your investigation, response, or notifications?
- Is there anything you would do differently next time?
- Do you need to make any updated to your incident response plan?

Do you have an incident response plan?

It is crucial for organisations to develop and maintain a plan to respond to privacy breaches that impact personal information they are responsible for. This includes personal information collected by, or shared with, third parties e.g., as part of a vendor or service provider contract. Where information is passed to a third-party service provider, the contract between the organisation should clearly set out the roles and responsibilities of each party when an incident occurs.

A privacy breach response plan will enable your organisation to respond quickly to a breach or incident, which can substantially decrease the impact on affected individuals, reduce the costs associated with dealing with a breach, and reduce the potential reputational damage to your organisation.

The plan should:

- Outline your organisation's plan for containing, assessing and managing the incident from start to finish.
- Include a clear description of roles and responsibilities.
- Include an audit function to ensure the plan is implemented and policies and procedures are reviewed regularly.
- Align with the organisation's security plan, privacy policy requirements, and any general incident management policies or processes.
- Be informed by data on previous near misses and any privacy and/or security breaches.

- Be tested in a mock scenario. Practice and refinement of the plan is key to its success.

Your incident response plan should be in a format that is concise and easy to follow. Make sure your employees know where the plan is stored and can access it easily. Your staff should also be familiar with the plan before they need to use it. This could be achieved by testing the plan in a simulated incident exercise, to give staff practice at putting the plan into action.

You should involve various business groups in the development of the plan, for example:

- Privacy function or team.
- Information security & IT.
- Risk and assurance.
- Operations.
- Senior management team.
- Communications.
- Legal.

Assigning roles and responsibilities

Understanding who does what in an incident will save time, avoid confusion, and provide employees with a clear picture of what they need to do. It also ensures that all required stakeholders are involved when they should be.

You will need to assign someone to the following roles when you assemble your incident response team:

- Coordinating the response – who leads the incident and is responsible for the decision making?
- Investigating the incident – who has the expertise to investigate the issue, contain it, and then take actions to prevent it reoccurring?
- Communicating with staff, affected individuals and stakeholders – who takes the responsibility for keeping staff updated as the incident progresses? Who will manage the external communications to affected individuals?
- Mandatory privacy breach notification – who makes the decision to notify OPC and who submits the notification?
- Debriefing the incident – who will lead a debrief of the incident, identify lessons learned, and any next steps?

These are all tasks that must be done, but you don't need a huge team of people to do them. However, you may wish to bring in experts to support the incident response team, particularly if you are a small organisation with a single person covering many of the response functions.

Prevent

While it's important to reflect on the lessons learned from privacy breaches and incidents, it's equally important to implement changes and improvements to prevent them from occurring.

See our Security and Internal access controls pou for guidance on some of the most common practices that can lead to data and privacy breaches if not appropriately monitored and managed within your organisation, and some of the preventative controls available to you.

Organisation examples

We've included some use cases based on fictional organisations to demonstrate each of the pou in practice. Read more about them in Introducing the Organisation Examples.

Large business – Fern Leaf

Fern Leaf holds a large volume of personal information. The Privacy Team works very closely with the Information Security team and together they run tabletop exercises to test potential breach scenarios and how to respond.

Fern Leaf regularly reminds its employees of the importance of spotting privacy breaches quickly. It runs training sessions and uses anonymised real-life scenarios to make the training more relatable. It reports regularly to senior management on trends they are seeing, and action taken to contain breaches.

If a breach is notifiable, the privacy team has a clear process on what information is required and the factors to consider. The Privacy Officer signs off on any notification to OPC and assists with drafting communications to impacted individuals.

Small business (charity) – Reach High

Reach High knows that a privacy breach would have a significant impact on client and stakeholder trust, which in turn would impact on its ability to deliver important services to at risk young people. For this reason, the Director of Support Services develops a simple Privacy Breach Management Plan to ensure that all breaches are recognised and managed properly. Reach High has decided that the most important thing to focus on is ensuring that all its employees can recognise a breach and know who to report it to. So, they complement the new plan with some targeted training that focuses on recognising and escalating breaches.

As a small organisation, breaches are managed by the leadership team as a group, with specific advice from the Director of Support Services. Breaches are recorded in the Privacy Risk Register, which the Director of Support Services uses to track resolution.

Start-up – Swiftstart NZ

Although the personal information Swiftstart NZ holds on its own behalf is reasonably minimal, it knows it has the potential to hold significant customer information within its platform on behalf of its clients, particularly as the company expands. It also knows that its clients have strong expectations around the security of the platform and will need to be immediately notified in the event of any breach to ensure the client company can take all appropriate steps (including making any required notifications).

The Operations Manager develops a privacy incident plan under which they will be the initial escalation point for any potential privacy incidents or near misses. They will undertake an initial investigation and assessment, including taking any appropriate immediate containment measures. Within 12 hours they will provide a report to the Swiftstart NZ founders with their assessment of the incident and recommended next steps, including whether notification to OPC and affected individuals is required or otherwise recommended. The founders endorse the plan and agree to commit to Swiftstart NZ's customers that any confirmed breaches where information is at risk will be notified within 24 hours of initial identification.

The founders recognise that ensuring speedy identification and escalation of any issues will be vital in order to meet their committed timeframe for client notification and decide to incorporate regular testing of the privacy incident plan by way of simulated incident into their routine digital readiness simulations. They also task one of their developers with creating an internal reporting tool so that any incidents can be easily logged by staff and pushed through to a log managed and maintained by the Operations Manager.

Small business (non-tech) – Green Gardens

The Administrator for Green Gardens develops a simple Privacy Breach Management Plan, which they run past the Owner/Manager, since accountability for privacy is shared between them. As a small business, breaches are managed by the Owner/Manager and the Administrator together, with the Administrator leading the response, including initial investigation, any notification requirements, and recording breaches in a privacy incident register.

Independent contractor – Jo Jones

Jo Jones develops a simple Privacy Breach Management Plan, which she has designed as a checklist for herself to go through whenever she thinks she may have identified a breach or near miss. Jo also has an Incident Register which is an excel spreadsheet where she records any breaches or near misses and the cause of them. When Jo is working for a community health service provider, Jo familiarises herself with their privacy breach management process, and knows who to escalate any incidents to, and where to record near misses.

Government agency – The Ministry

The Privacy team uses the relationships it has built with the Ministry's IT and information management team through its collaboration on data inventory, to work more closely together on breach management. All teams understand that breaches that affect one team are likely to impact or be relevant to others. The teams work together to develop a breach response plan. They then trial and test the plan in a mock privacy breach scenario with SLT members so they know what to expect should a serious breach happen. The team has also established clear escalation pathways for breaches that customer service becomes aware of, so that issues are promptly identified and acted upon.