Serious breach notification
four months in

Privacy breaches cause real harm to the people affected.

- More than half of the serious privacy breaches reported to our office involved emotional harm, and around one third resulted in a risk of identity theft or financial harm. Some breaches can cause more than one type of harm to the individuals affected.

<table>
<thead>
<tr>
<th>Percentage of breaches involving:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Emotional harm</td>
<td>65%</td>
</tr>
<tr>
<td>Financial harm</td>
<td>30%</td>
</tr>
<tr>
<td>Reputational harm</td>
<td>30%</td>
</tr>
</tbody>
</table>

- At this early stage in mandatory reporting, a high number of reports from one sector doesn’t necessarily mean poor privacy practice – it may mean these sectors are more aware of their obligations to report.

Breaches can occur in any sector – public, private, or non-profit. We have had breaches reported from the social assistance sectors, financial and insurance services, education and training, retail trade and accommodation, and even mining.

- Consistent with a long-standing pattern, email errors are the most common type of privacy breach reported to our office. They’re easy to prevent with training and the right procedures.

Be careful when including personal information in emails, double check attachments, have a send delay and use Bcc when sending to multiple recipients.

- Over three quarters of serious privacy breaches reported to our office involved information that was likely to be sensitive. Remember, the personal information you collect and use is incredibly important to people and can cause serious harm if it gets into the wrong hands.

<table>
<thead>
<tr>
<th>Sensitivity of information breached</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensitive or likely sensitive</td>
<td>84%</td>
</tr>
<tr>
<td>Not likely sensitive</td>
<td>9%</td>
</tr>
<tr>
<td>Don’t know</td>
<td>7%</td>
</tr>
</tbody>
</table>

Organisations must report serious breaches as soon as they practically can. Don’t take a ‘wait and see’ approach.

Within 2 days: 33% Serious breaches reported to OPC
Within 5 days: 54%

Personal information is sensitive

- We have seen a 97% increase in the number of breaches reported to us in comparison to the preceding six months.

What we’re doing

Reporting serious privacy breaches to the Privacy Commissioner became mandatory on 1 December 2020. There were 76 serious privacy breaches notified to us between 1 December 2020 and 31 March this year.

Compliance

For the first six months of the Privacy Act 2020, our office has been focused on educating organisations and businesses to help them understand their new legal responsibilities. When you report a privacy breach to us, we want to help you make it better!

The Privacy Commissioner does have powers under the Privacy Act to enforce compliance when organisations repeatedly fail to meet their obligations or should know better.

For example, if breaches generated by email errors persist in organisations that are not taking the necessary precautions, we are prepared to use enforcement action to support behaviour changes.

Be prepared

- Protect the personal information you hold – privacy is precious!
- Learn from privacy breaches and near misses. Change practices to stop the same mistakes from happening again.
- Have a privacy breach plan.

Use our NotifyUs tool to report serious privacy breaches to us as soon as you can.

Reporting Serious Breach
To MANA Matatapu

Te Mana Matatapu

Privacy Commissioner