

own
your
online

The webinar will start shortly...



Privacy Commissioner
Te Mana Mātāpono Matatapu

own
your
online

Data breach readiness: What every business should know

Our presenters



Tom Roberts – National Cyber Security Centre

Team Leader, Response and Investigations



Susan Allen – Office of the Privacy Commissioner

Manager, Compliance and Enforcement

Today's agenda

- What is a data breach and how it can happen
- Legal requirements under the Privacy Act, including when and how to report.
- What an effective incident response looks like.
- Practical steps to improve your organisations preparedness and incident response.

About the National Cyber Security Centre

The NCSC is the Government's lead agency for cyber security.

- We provide advice and education to all New Zealanders, from businesses to individuals to nationally significant organisations.
- We also provide incident response and support to anyone who needs it.
- The [Own Your Online](#) website has easy to understand resources and guides to help educate all New Zealanders about cyber security and stay ahead of the latest scams and threats.

What is a data breach?

A data breach happens when private information held by an organisation is compromised, stolen or released by accident.

The full extent of the Qantas cyber attack has been revealed with 5.7m customers affected



Alan Granville

July 9, 2025 - 12:37pm

→ Share



Qantas CEO Vanessa Hudson said the airline would be reached out to affected customers.

NEW ZEALAND / BUSINESS

Supermarket loyalty card cyberattack prompts password warning

9:21 pm on 12 July 2025

Share this



How does it happen?

Data breaches can happen because of an intentional attack or unintended error.

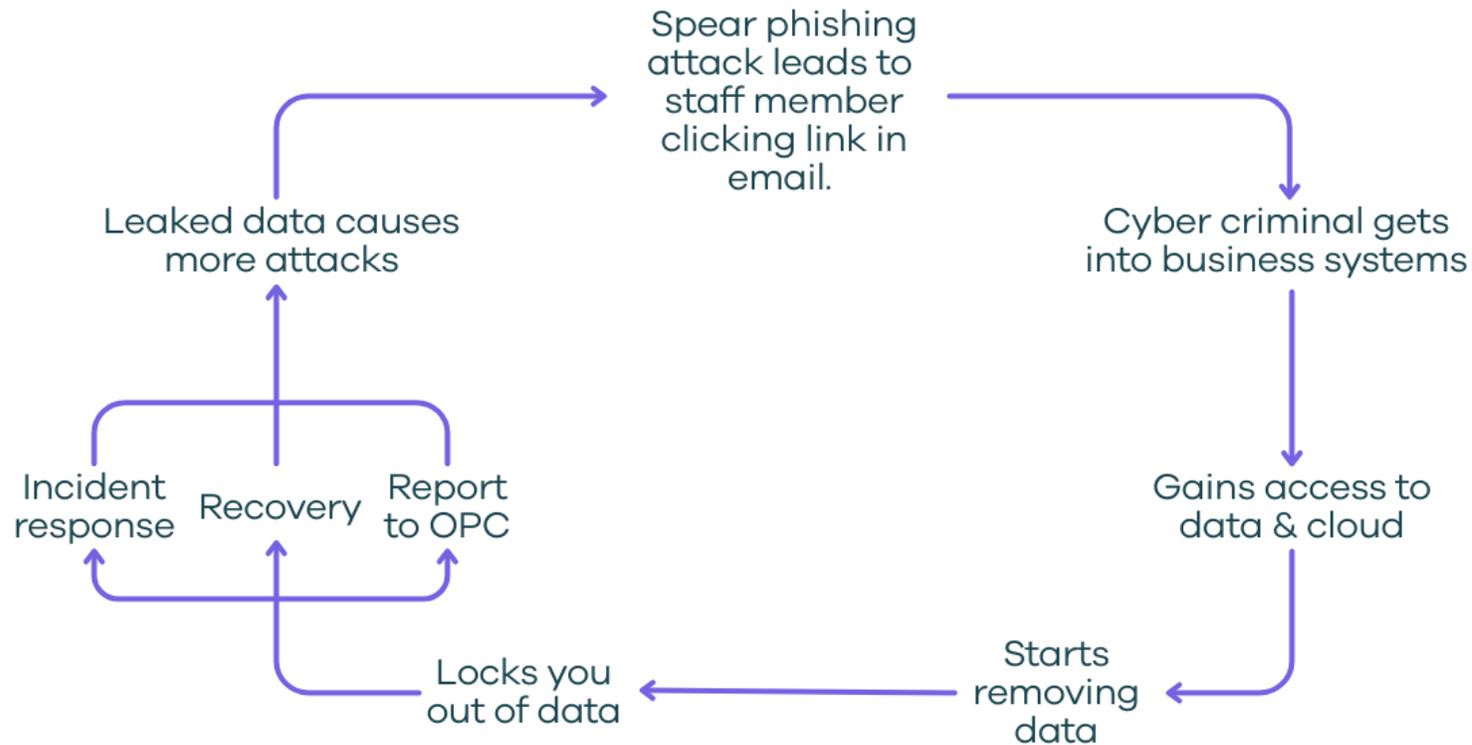
- Cybercriminals can exploit vulnerabilities in systems or networks to access your data.
- Someone in your organisation may be targeted in a phishing attack and tricked into revealing important information, such as their login details.
- Insider threats can be a source of a data breach. Anyone with authorised access could misuse their privilege or intentionally leak information.
- Data can also be leaked through human error, such as in an email to the wrong person, or through misplaced or stolen devices containing sensitive information.

What effect does it have?

A data breach can affect your organisation in many ways.

- **Financial:** your organisation could incur costs such as legal fees, penalties and the cost of remediation.
- **Reputational:** a data breach can erode customer trust and affect brand credibility.
- **Legal:** if you are a business owner, you are obligated by the Privacy Act 2020 to protect peoples' personal data and to report breaches promptly.
- **Personal:** stolen personal data can lead to identity theft, financial fraud, and other malicious acts.
- **More phishing:** people whose information has been leaked may become the target of more phishing attacks

Common scenario



What happens to the data?

breachforums.cx

2 hours ago (This post was last modified: 1 hour ago by OneERA) #1

Hey folks, we've recently acquired information on about 2.5 million New Zealand citizens from [REDACTED].co.nz]. We initially planned to sell this data, setting the price for a copy of the data at \$30,000. However, due to our high asking price, no one was willing to buy. We believe we just haven't encountered hackers who understand how to utilize this data. Now, we've decided to release this data for free, allowing anyone to use it for whatever purposes they desire. Enjoy the leaked data, hackers!

Note: Another exciting piece of news is that we will continuously monitor and steal data leaks from [REDACTED].co.nz] and release them for free here. Stay tuned!

The data we've successfully stolen includes:

Citizens' names, home addresses, mobile numbers, email addresses, dates of birth, home phone numbers, postal codes, genders, UserIds. Private information of citizens, including some questionnaire answers, as well as some citizens' videos and musical materials. Some voting information - [REDACTED] - The [REDACTED]

...

[https://files.fm/u/\[REDACTED\]](https://files.fm/u/[REDACTED])
[https://files.fm/u/\[REDACTED\]](https://files.fm/u/[REDACTED])

[https://pixeldrain.com/\[REDACTED\]](https://pixeldrain.com/[REDACTED])
[https://pixeldrain.com/\[REDACTED\]](https://pixeldrain.com/[REDACTED])

password:

487 million whatsapp users database
Wednesday November 16, 2022 at 05:23 AM

Hi, Today I'm selling following Whatsapp users database of recent 2022 updated. You'll get very recent mobile numbers of users.

Total countries are upto 84
Total Estimated records - 487 million plus
Telegram link - [https://t.me/\[REDACTED\]](https://t.me/[REDACTED])

Sr # Country Records

1	Afghanistan	558,393
2	Africa	14,323,766
3	Albania	506,602
4	Algeria	11,505,998
5	Argentina	2,347,553
6	Australia	1,249,388
7	Australia	2,203,478
8	Bahrain	1,450,124
9	Bangladesh	3,816,339
10	Belgium	3,183,584
11	Bolivia	2,959,209
12	Brazil	8,064,916
13	Brunei	213,795
14	Bulgaria	432,473
15	Cameroun	1,997,658
16	Canada	3,494,385
17	Chile	6,899,083
18	China	670,334
19	Colombia	17,957,908
20	Costa Rica	1,464,002
21	Croatia	659,115
22	Cyprus	152,321
23	Czech Republic	1,375,988
24	Denmark	639,841
25	Ecuador	310,259
26	Egypt	44,823,547
27	Finland	1,581,569
28	France	19,848,559
29	Germany	6,054,423
30	China	1,027,669
31	Greece	617,722
32	Guatemala	1,415,018

[REDACTED] Friday September 23, 2022 at 01:12 AM

4 hours ago

Hello [REDACTED]

Lots of news. [Optus](#) announced database leak. Here we have leaked data.

Data come in 2 files:

11,2m Users
Data included email, date of birth, first last name, mobile number, identification numbers (such driving license), subscriptions if available (mobile postpaid, mobile prepaid, broadband), and more

4,232,652 have form of identity document number
3,664,598 of them are Driving Licence number
4,342,276 have active subscription (multiple subscription can be included, this is just line count)
6,577,020 mobile subscriptions (mixed prepaid postpaid)
4,033,403 NO_EMAIL, user data still valid however

100 sample [REDACTED]

10m Addresses
Data included email, full name, date of birth, gender (Mr Mrs), mobile number, address, identification numbers (such driving license) and more

3,817,197 have form of identity document number
3,238,014 of them are Driving Licence number
4,031,503 NO_EMAIL, user data still valid however

100 sample [REDACTED]

[Optus](#) if you are reading! price for us to not sale data is 1,000,000\$US! We give you 1 week to decide.

Buyers, price for users data 150,000\$US, price for addresses data 200,000\$US. Together 300,000\$US. Exclusive sale cost 1,000,000\$US total. No sale will be made for 1 week until [Optus](#) reply.

All payment will be in Monero.

What happens when you notify OPC of a breach?



Susan Allen, Compliance & Enforcement Manager

19 August 2025

If you remember nothing else from this presentation, remember this:

- Your agency has legal obligations under the Privacy Act.
- The Office of the Privacy Commissioner has a LOT of guidance at www.privacy.org.nz to help you identify and understand these obligations.

Who are we?

- We are an independent crown entity tasked with working to develop and promote a culture in which personal information is protected and respected.
- Dispute resolution
- Compliance
- Policy
- Capability & Guidance
- Legal



What do we do?

- Investigating privacy complaints from the public
- Issuing codes of practice
- Education, publicity, guidance and training
- Oversight, compliance and monitoring
- Consultation and policy advice
- Acting as an intervenor in the courts on privacy issues

Defining a privacy breaches

A privacy breach is:

Unauthorised or accidental access to, or disclosure, alteration, loss, or destruction of, the personal information; or

An action that prevents the agency from accessing the information on either a temporary or permanent basis

Some are notifiable:

A privacy breach that has caused, or is likely to cause, **serious harm** to an individual is a notifiable privacy breach

If a notifiable breach occurs:

Legally required to notify the Commissioner as soon as practicable

Must notify affected individuals as soon as practicable, unless an exception applies

Information may be provided incrementally

Obligation of secrecy

Breach management

Contain

Reduce the impact

Assemble response team

Diagnose what happened

Secure the information



Assess

How successful is the containment?

Sensitivity of the information

Is there a malicious element?

What is the context?

Document your decision making

Consider your regulatory obligations

Notify

Be transparent, and prompt to reduce harm

Notify OPC:

- Information may be provided incrementally
- Obligation of secrecy

[Home](#) / [Your responsibilities](#) / [Privacy breaches](#) / [NotifyUs - For organi...](#)

NotifyUs - For organisations to report privacy breaches

[Do I need to notify? →](#)

If you have already determined that a privacy breach at your organisation is notifiable, or wish to notify us in any case, click on the 'Report a breach' button below to be taken to NotifyUs.

See a checklist of what information is required [here](#).

Please note: NotifyUs works best with up-to-date internet browsers (e.g. Chrome, Firefox and Edge). We recommend not using legacy browsers with it (e.g. Internet Explorer and legacy Edge).

[Report a breach →](#)

If you need to update a privacy breach report you previously submitted to us, you can:

Email your update to: notifyus@privacy.org.nz

Or use this form:

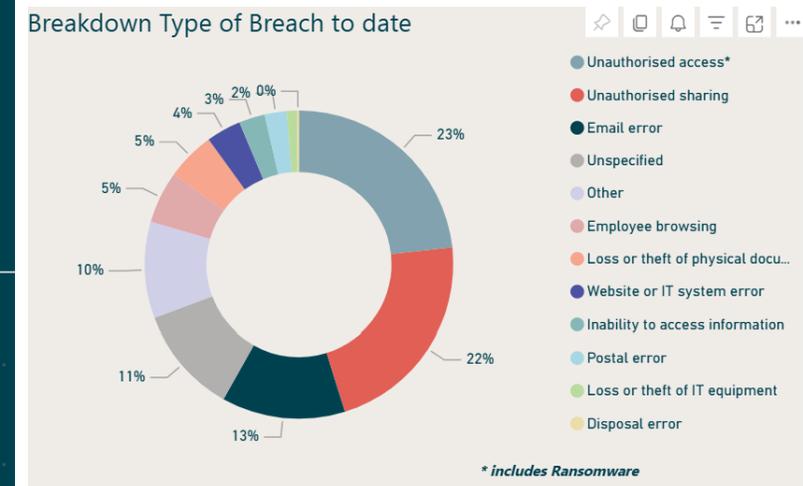
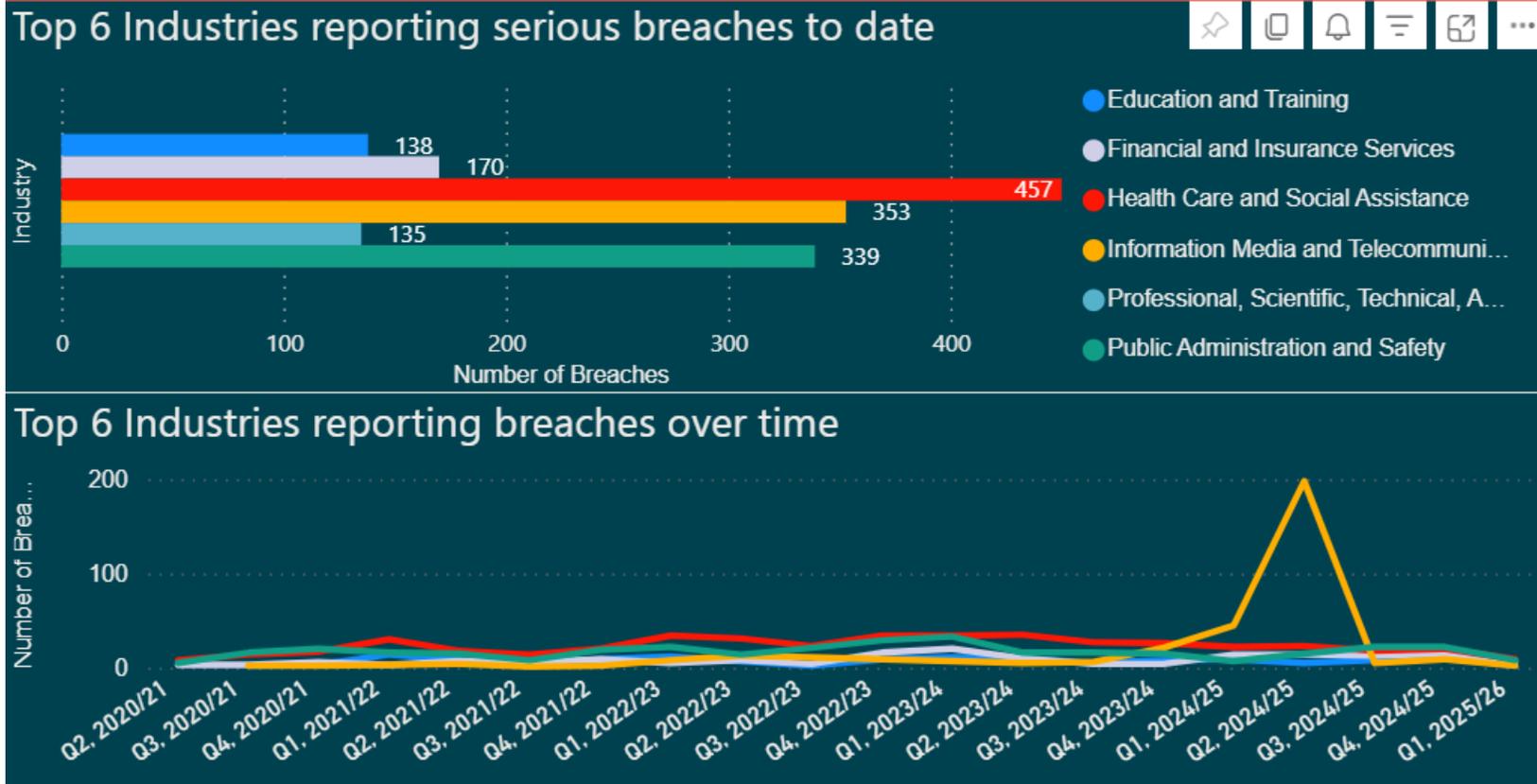
[Update a breach →](#)

What we'll ask you:

- Contact details
- Timeline of the incident
- What happened
- What type of information is involved
- Likely harm to individuals
- Affected individuals

Information may be provided incrementally

Privacy breaches reported to us



Questions to ask yourself and your team

What personal information do we hold? What are we collecting, and why?

Who is my agency's privacy officer, and how do I raise privacy concerns?

Do I know what we have in our privacy policy? What am I telling individuals when I collect their personal information?

Do our information handling practices line up with what we're telling people?

What steps can I take to keep information secure?

Does my agency hold information that we don't need anymore?

What happens if something goes wrong? Do we have a breach management plan?

What are my privacy blind spots? Where can I go to learn more?

Guidance hub: <https://www.privacy.org.nz/responsibilities/poupou-matatapu-doing-privacy-well/>



Thank you – any questions?





How to protect your business from a data breach

Data collection, storage and encryption

Data collection

Consider what information you really need to collect from clients and contacts. Your level of risk is based on the amount of data you have — the more you collect, the more valuable it is to an attacker. By only collecting what you need, you reduce your risk.

Data storage

If you use a cloud service for data storage, check the provider can give you the services and protection you need.

Encryption

Make sure you're encrypting any data you collect. This includes while it's:

- in transit – for example, collect data from your customers through an HTTPS form
- at rest – when it's stored in a database.

Manage staff access

We often use the term 'principle of least privilege'. This means only giving people the level of access they need to do their job.

This reduces the risk of data being accidentally shared. It's also important to make it clear to employees who have access to data that they can only use it for work-related purposes.

Create an incident response plan

Develop a response plan for what to do if your business is affected by a data breach – or any other type of online security incident. Make sure your staff know to report any security breach to your IT person or team.



Incident response to a data breach

If your business has had a data breach:

- disconnect the compromised system from the internet, but don't turn it off. If you turn it off, you could lose evidence that will help you work out what happened
- reset the passwords for any compromised accounts.

Key takeaways

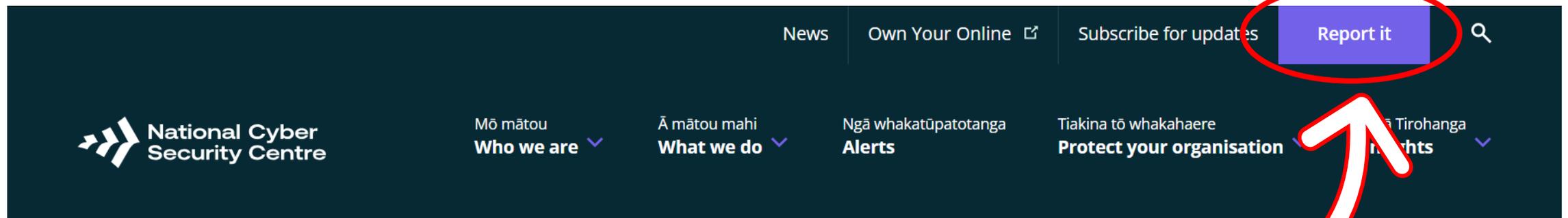
- Data breaches are easier to avoid than they are to fix. Having the right protections in place is key.
- The effects of a data breach can go on for years.
- Your business has legal obligations under the Privacy Act.
- OPC can help you figure out what your obligations are in the event of a data breach.
- Always be conscious of what data and information your business collects.
- If you have a data breach, report it and get assistance.

Getting help

How to get in touch with NCSC

If there is a cyber security incident:

- Website: [Report it](#)
- Phone: 0800 114 115
- Email: incidents@ncsc.govt.nz
- General enquires: info@ncsc.govt.nz



REMINDER: If you remember nothing else from this presentation, remember this:

- Your agency has legal obligations under the Privacy Act.
- The Office of the Privacy Commissioner has a LOT of guidance at www.privacy.org.nz to help you identify and understand these obligations.

Thank you and sign up to Cyber Smart Week

6 – 12 October