

Porter Novelli Australia

Cyber Incidents:
Preparation, Reputation & Response

9 March, 2023

Imagine you're the CEO of Medibank...

13,000 policy holders lost in the December quarter

More to come as renewals come through

\$1.8 billion in market capitalisation lost

Market Summary > Medibank Private Ltd

3.28 AUD

-0.40 (-10.87%) ↓ past 6 months

23 Feb, 4:10 pm AEDT • Disclaimer

+ Follow

1D | 5D | 1M | 6M | YTD | 1Y | 5Y | Max



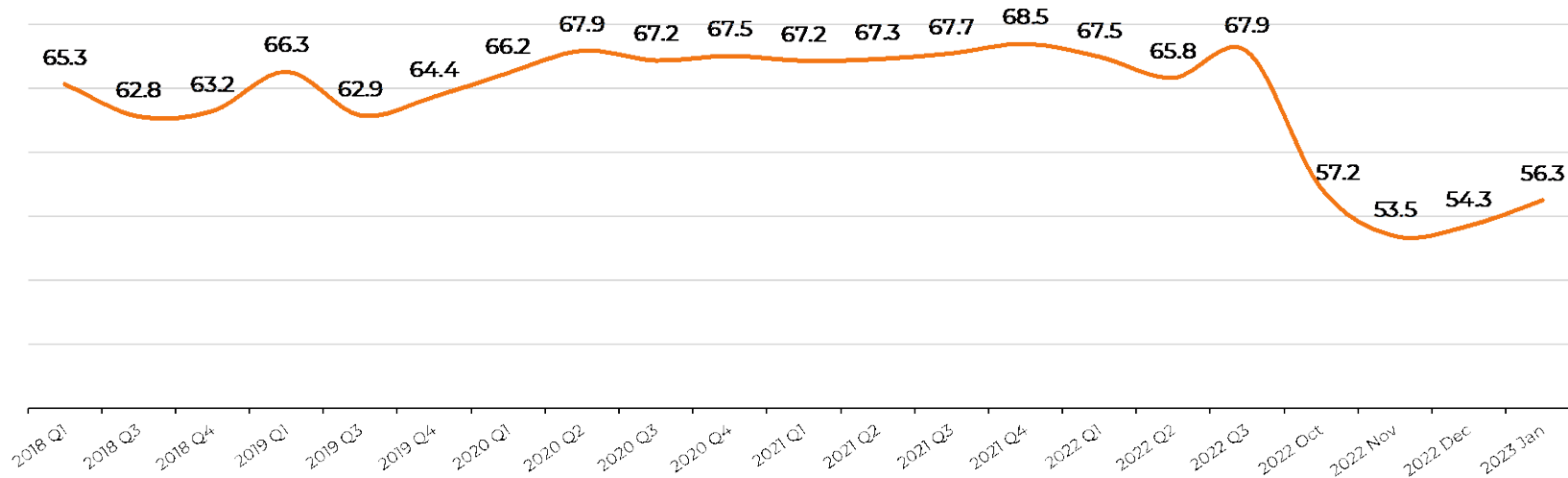
Open	-	Mkt cap	9.03B	52-wk high	3.78
High	-	P/E ratio	22.93	52-wk low	2.73
Low	-	Div yield	4.09%		

[More about Medibank Private Ltd](#) →

[Feedback](#)

Reputational impact of recent Cyberattacks & Data breaches

Optus/Medibank Reputation Average Trended



Q1: Jan-Mar; Q2: Apr-Jun; Q3: Jul-Sep; Q4: Oct-Dec

Now imagine you...

..are about to embark on an international student recruitment campaign.

..are in the middle of a contentious EA negotiation with your staff.

..are about to begin a major fundraising campaign.

..lose thousands of personal student records and in employee payroll data in the lead-up to key enrolment periods.

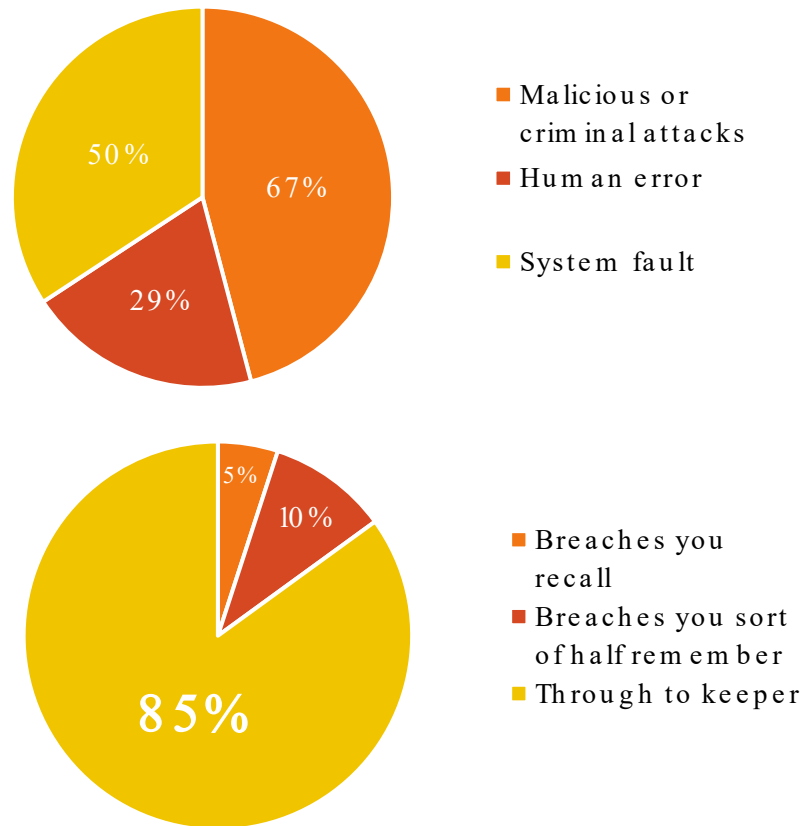
..lose the ability to access your network for a week when offers are going out to school-leavers.

Most breaches go through to the keeper...

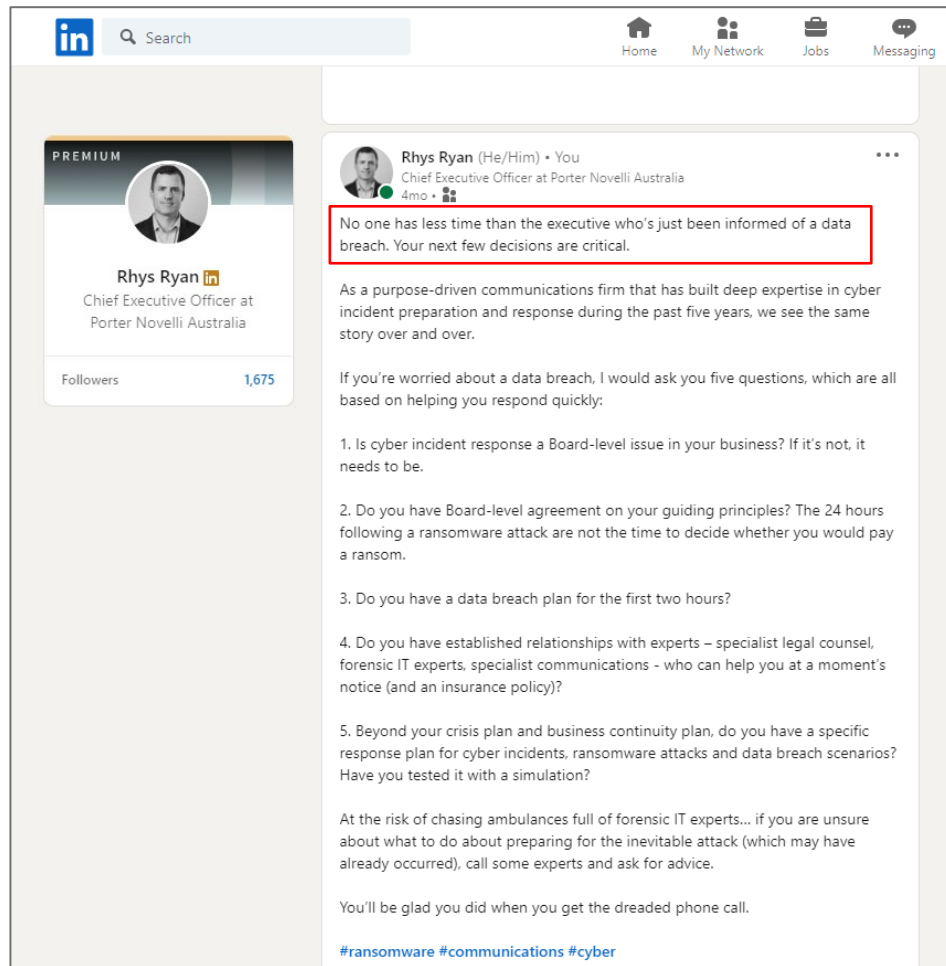
- Non-salacious circumstances
- Non-clickable brand names
- Handled well
- Not overly sensitive data
- Happen on a Friday afternoon when journos already at pub (seriously)...

But when handled badly...

Notifiable data breaches – Jan - Dec 2022





Never a truer word spoken...



LinkedIn Search Home My Network Jobs Messaging

PREMIUM

Rhys Ryan 
Chief Executive Officer at Porter Novelli Australia
1,675 Followers

Rhys Ryan (He/Him) • You
Chief Executive Officer at Porter Novelli Australia
4mo • 

No one has less time than the executive who's just been informed of a data breach. Your next few decisions are critical.

As a purpose-driven communications firm that has built deep expertise in cyber incident preparation and response during the past five years, we see the same story over and over.

If you're worried about a data breach, I would ask you five questions, which are all based on helping you respond quickly:

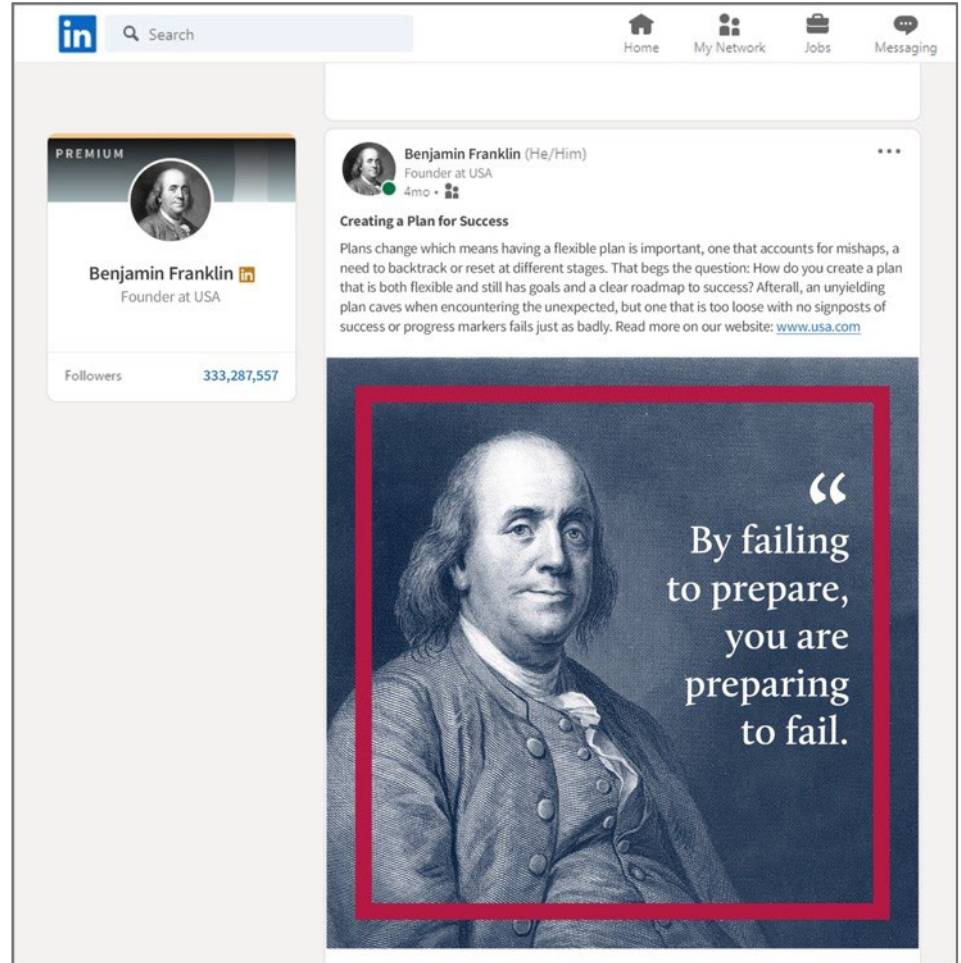
1. Is cyber incident response a Board-level issue in your business? If it's not, it needs to be.
2. Do you have Board-level agreement on your guiding principles? The 24 hours following a ransomware attack are not the time to decide whether you would pay a ransom.
3. Do you have a data breach plan for the first two hours?
4. Do you have established relationships with experts – specialist legal counsel, forensic IT experts, specialist communications - who can help you at a moment's notice (and an insurance policy)?
5. Beyond your crisis plan and business continuity plan, do you have a specific response plan for cyber incidents, ransomware attacks and data breach scenarios? Have you tested it with a simulation?

At the risk of chasing ambulances full of forensic IT experts... if you are unsure about what to do about preparing for the inevitable attack (which may have already occurred), call some experts and ask for advice.

You'll be glad you did when you get the dreaded phone call.

[#ransomware](#) [#communications](#) [#cyber](#)

Or an actual
proverb...



Today...

1. Brief defining of terms
2. When you need to call for back-up
3. Trends and changes we're seeing
4. Best practice in preparation
5. Best practice in response
6. What to consider in recovery

Quick show of hands...



The Notifiable Data Breach Scheme

A breach is notifiable if it is eligible (i.e., meets the criteria set in the Privacy Act) -

- Has a security breach resulted in - or may result in - unauthorised access, use or disclosure of personal information (or was personal information lost or misused)?
- Are the affected individuals at risk of serious harm?
- Is remedial action available? If so, can the action remove the risk of serious harm?
- Some organisations are also subject to sector-specific incident reporting obligations (e.g., Prudential Standard CPS 234, and Security of Critical Infrastructure Act 2018).

Don't forget B2B contractual obligations

Always important to review contractual obligations on notifying any cyber incidents

- These sorts of obligations are increasingly common
- They prevent a contractor from using discretion to determine whether the incident is a notifiable data breach
- Most clauses will require the other side to cooperate on the assessment and remediation of the breach and permit them to take responsibility for reporting the breach
- A supplier/service provider contract may also require you to have insurance in place, as well as any limitations or exclusion of liability that might apply

GDPR Fines Tracker & Statistics

Total Number of GDPR Fines

340

Total Amount of GDPR Fines

€ 158,135,806

And GDPR...



Smallest Fine

€ 90

Hospital on
Nov 18, 2019
Hungary



Largest Fine

€ 50,000,000

Google Inc. on
Jan 21, 2019
France

Why am I here?

We're not required for every incident.



BREAK GLASS
IN CASE OF
EMERGENCY

Why am I here?

We're not required for every incident.

Sometimes we're just advisors...



Why am I here?

We're not required for into every incident.

Sometimes we're just advisors...

But sometimes there is a **LOT** of wood to chop.



Why am I here?



Australian Government

**Office of the Australian
Information Commissioner**

VS



Why am I here?

We're not required for into every incident.

But some need more help...

- Listed entities

ASX Announcement

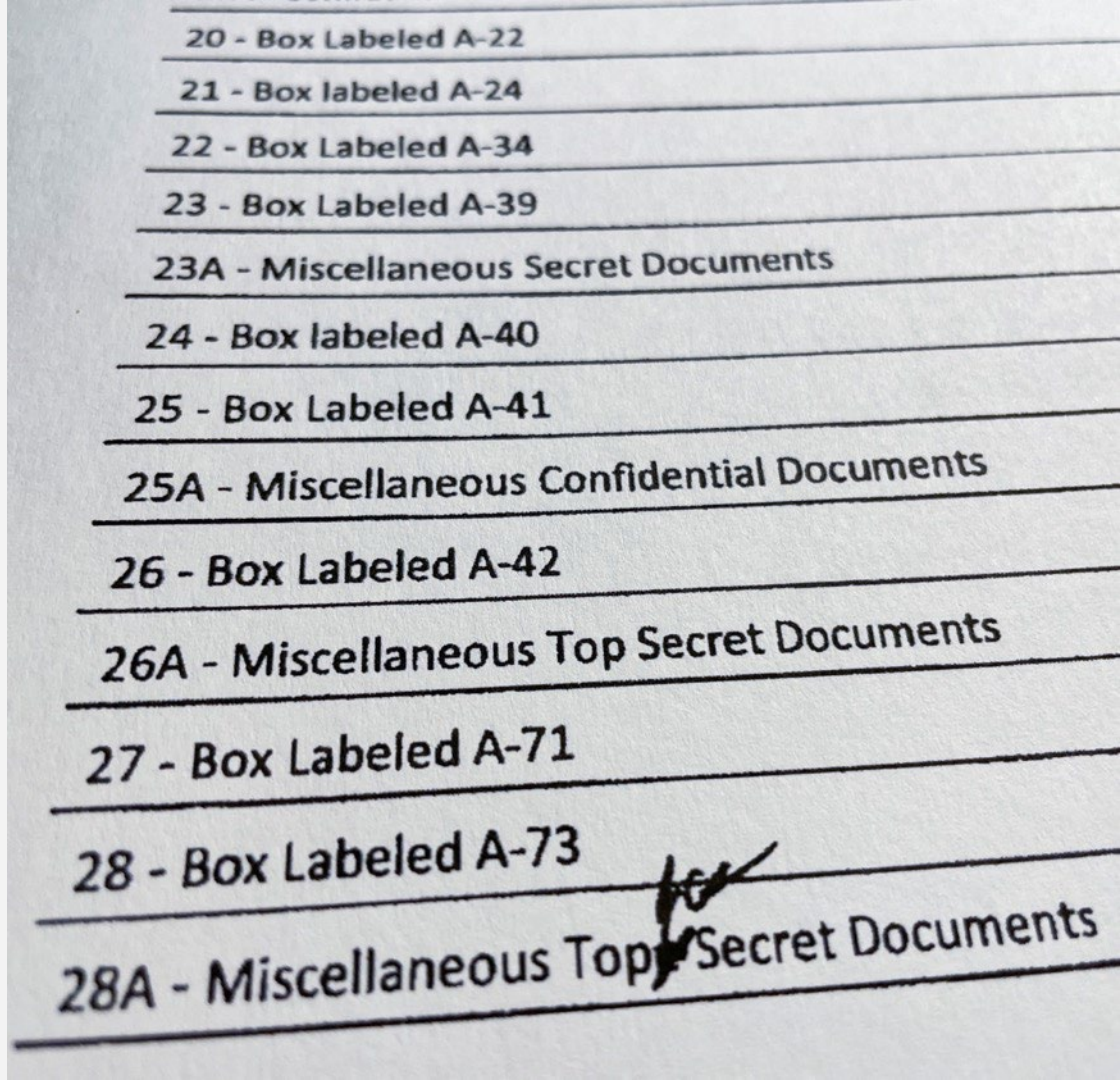
Trading Halt Request

Why am I here?

We're not required for into every incident.

But some need more help...

- Listed entities
- Highly sensitive situations

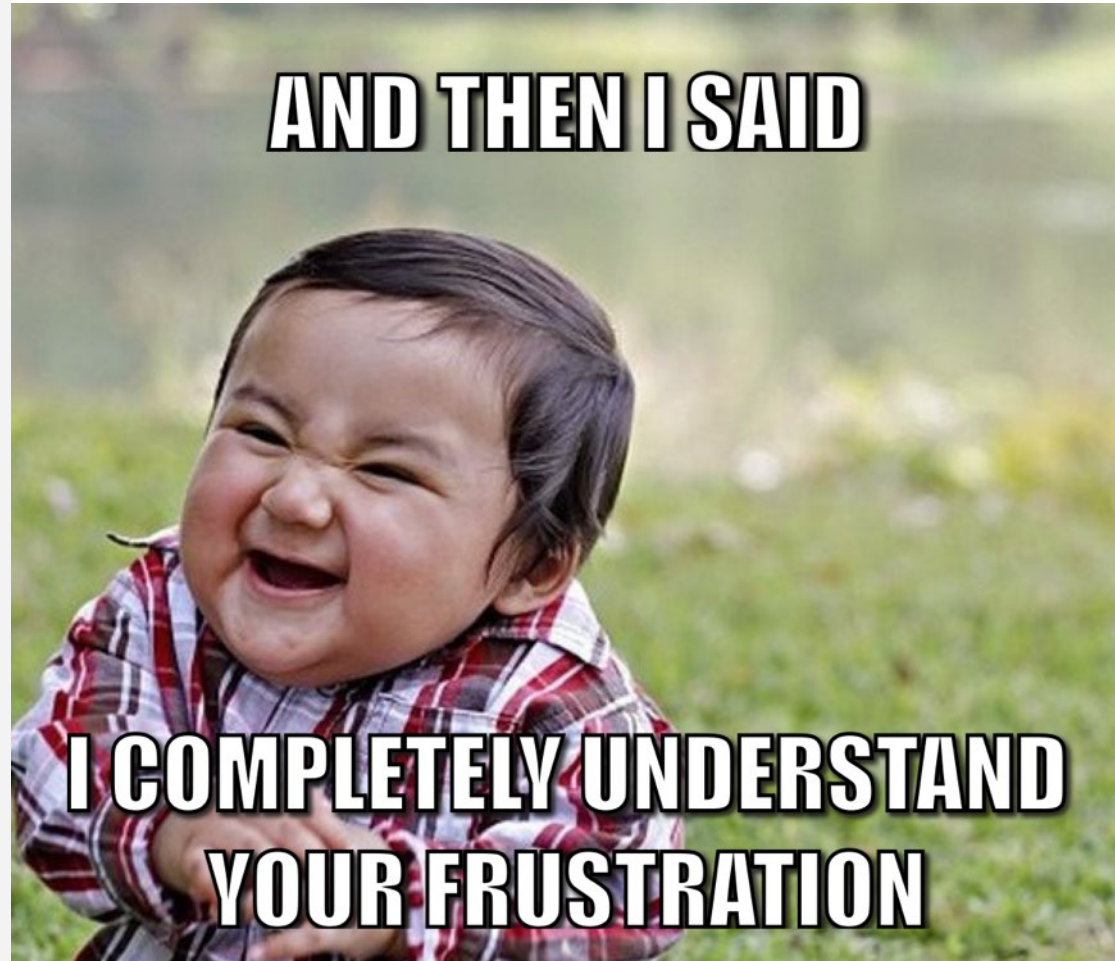


Why am I here?

We're not required for into every incident.

But some need more help...

- Listed entities
- Highly sensitive situations
- B2B with complex breaches



Why am I here?

We're not required for into every incident.

But some need more help...

- Listed entities
- Limited expertise; limited resources
- Highly sensitive situations
- B2B with complex breaches

And...

- The Valley of Uncertainty

"We can say definitively that there is no evidence that customer data has been removed from our systems..."

The Valley of Uncertainty



"Our investigation has been ongoing and as these incidents continue to evolve..."
"....previous statements had been very clear that they were point-in-time updates."

Business & Gov Residential

Sensitive Data

Lost



Lostock, NSW 2311

Lost River, NSW 2583

20 minutes?

Sheesh.

No small talk?

It's Your ABC, indeed.

Hello,

I've been informed that you have been the subject of a hack.

Is this the case?

Have you identified the culprit?

Who has been affected?

How many customers have been affected?

Have you advised customers of the hack?

How large is this hack?

Is any information being held to ransom, and if so what is your position on this?

Has this affected your systems or operations?

Has any sensitive information been accessed, like payment details or personal records?

Will you be advising the OAIC of the data breach?

My deadline is rolling.

Preparation and training is key.

- Audits and reviews of data breach response plans
- Crisis simulations with executive teams and boards
- You must have a playbook.

..and cue training montage.



Ransomware attacks are more targeted

Key trends we're seeing

- Companies with highly sensitive data
- Household names
- B2B companies in highly competitive sectors
- Insurance policies
- Companies that can pay

..and more government intervention...



THE  AGE

Cybersecurity to get national supervisor in wake of hack attacks

Monday 27 February 2023

Preparation: Nine Things

1. Specific Data breach plan (BCP)
2. Simulations
3. A culture of safety
4. Scorched earth on old data
5. To insure or not to insure
6. To pay or not to pay
7. Established relationships
8. Single source of truth
9. Contractual obligations



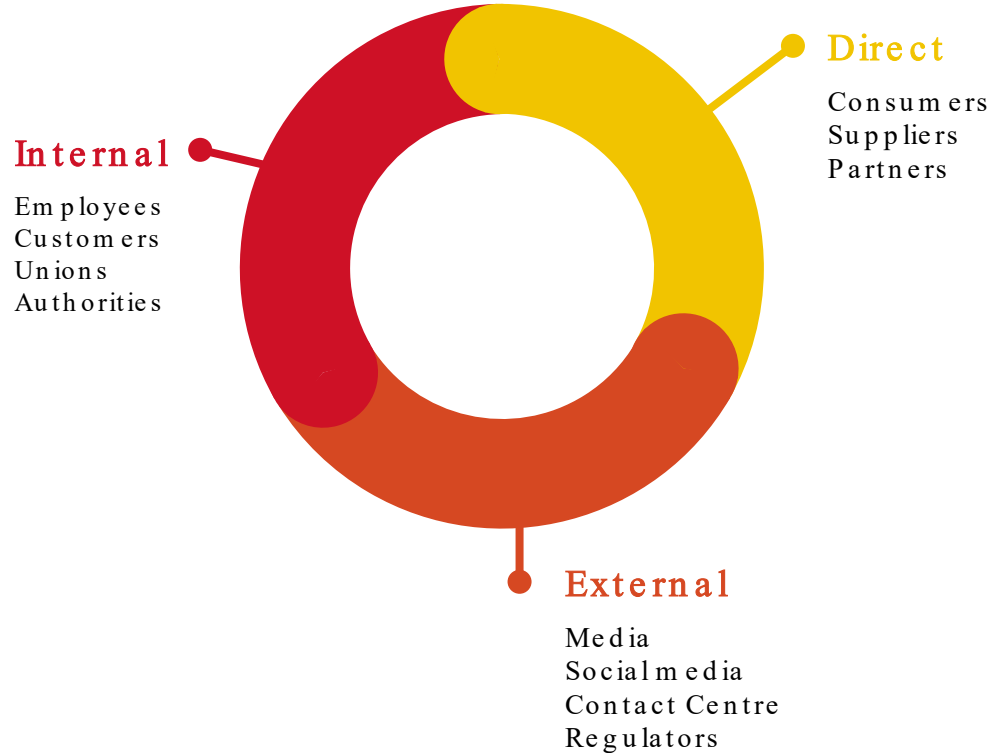
Response: Be transparent..ish

1. Guiding Principles: Do the right thing NOW



Response: Be transparent..ish

1. Guiding Principles: Do the right thing NOW
2. Narrowcast to stakeholders before the media does



Response:

Be transparent..ish

1. Guiding Principles: Do the right thing NOW
2. Narrowcast to stakeholders before the media does
3. The investigation is ongoing. Flood the zone: Say something, but just don't say anything

Response: Be transparent..ish

1. Guiding Principles: Do the right thing NOW
2. Narrowcast to stakeholders before the media does
3. The investigation is ongoing. Flood the zone: Say something, but just don't say anything
4. Don't play the victim ..but...

A portrait of Clare O'Neil MP, a woman with blonde wavy hair, wearing a red blazer, speaking outdoors. The background is blurred green foliage.

“The information at stake here is personal, private health information of Australian citizens...

If anything happens to put this into the public realm, it will be an absolute dog act.

Response: Be transparent..ish

1. Guiding Principles: Do the right thing NOW
2. Narrowcast to stakeholders before the media does
3. The investigation is ongoing. Flood the zone: Say something, but just don't say anything
4. Don't play the victim ..but...
5. Look after your people

There is no Dad Joke here. You really will need to genuinely look after your people.

Data breaches are very traumatic.

Recovery: what to consider

- Separate teams for response and recovery
- Commit to change and go above and beyond
- Document change

..and become a small target...



In summary

Lack of speed kills.

Be careful what you say.

Get good advice.

Do the right thing.

**PORTER
NOVELLI** 

50 YEARS