PORTER NOVELLI | Quantum Market Research

Cyber Security Incidents:
A Call to Action

2023

Every Australian organisation will be impacted by a cyber security incident at some point.

While several cyber security incidents have made headlines during the past two years, many people are not aware that there were approximately 1300 notifiable data breaches reported to the Office of the Australian Information Commissioner (OAIC) from January 2022 to June 2023.

These incidents affected millions of Australians.

As Australia's leading communications firm in cyber incident response and preparation, Porter Novelli has worked on hundreds of these incidents in recent years.

This led us, in partnership with Quantum Market Research, to research the impact of these incidents on the Australians who are affected by them.

1300
notifiable breaches reported from January 2022 to June 2023

This study provides insights into three key areas:

1. The **expectations** of Australians around organisations' data security
2. Their views on the **effectiveness of communications** and support from impacted organisations
3. How cyber security incidents impact **consumer trust** and **purchase behaviour**.

We are sharing these insights to highlight the need for organisations to prioritise customer and employee experience in a cyber security incident.

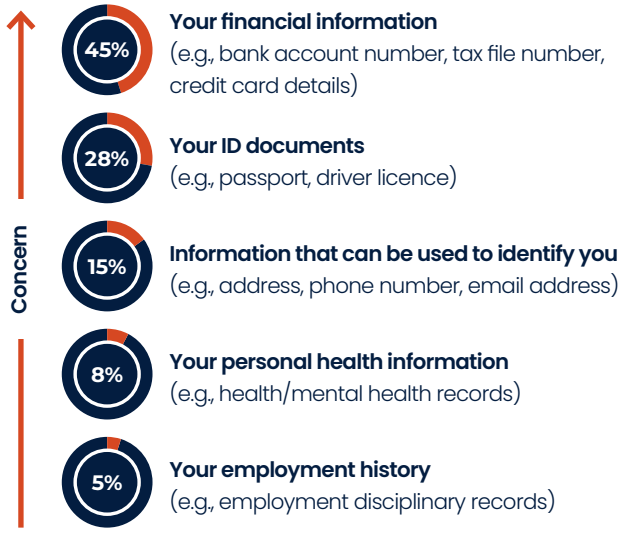
This goes beyond best-practice, which includes direct, transparent communications with their customers, consumers, staff, and stakeholders in line with core values.

We believe organisations need to actually support individuals impacted by an incident more effectively.

The key challenges

As the Australian Prudential Regulation Authority (APRA) urges the financial sector to raise the bar on data protection, Australians reveal they are more worried about losing banking details than their ID or health information.

Australia's financial institutions are not doing enough to prevent attacks according to APRA, whose recent study has revealed gaps across the industry. At the same time, the study found almost half of Australians (45%) are more concerned about losing their financial information than any other information.



Australians are increasingly concerned about being affected by a cyber security incident.

From November 2020 to July 2023, the number of Australians concerned about cyber crime climbed from 62 per cent to 74 per cent.

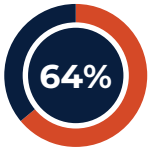
This concern is here to stay, with 82 per cent of Australians saying they are more concerned about the security of their personal information than they were five years ago.

The number of Australians being targeted is on the rise. Half of Australians (51%) say they are frequently targeted by cyber-related scams. Even more expect to be targeted in the next year (57%).

of Australians believe it's likely they will be impacted by an incident in the next 12 months

are taking measures to protect their personal data

feel that organisations aren't doing enough to protect their personal information



agree that organisations can securely protect their personal information

Australians are sceptical that our institutions protect them from hackers, and trauma from previous cyber security incidents is driving feelings of helplessness.

More than half of Australians (57%) believe it's likely they will be impacted by an incident in the next 12 months, despite the fact that most Australians (77%) are taking measures to protect their personal data.

Almost three in five (59%) feel that organisations aren't doing enough to protect their personal information from hackers. This is especially true for customers who have already been impacted by a cyber security incident (51%).

Consumers believe organisations are complacent (not proactive) in their prevention and response to a cyber security incident, with 78 per cent of consumers concerned about how organisations manage their personal data.

While 64 per cent of Australians agree that organisations can securely protect their personal information, just 41 per cent believe that organisations are actually doing enough, showing that most organisations are not living up to consumer expectations.

Millions of Australians think they should have been told about cyber security incidents, but weren't.

One-fifth (21%) of Australians know that their data was held by organisations that suffered major breaches, but they weren't notified as to whether or not their data was impacted.

This appears to justify the concerns of the 59 per cent of Australians who believe most organisations aren't doing enough to protect them.

One in 10 (9%) had to take time off work due to a cyber security incident

The cost of a cyber incident is greater than just financial.

In addition to the financial distress caused by cyber security incidents, Australians experience social and emotional impacts. Nearly half of Australians (48%) reported experiencing emotional distress as a direct result of a cyber security incident, and one in 10 (9%) had to take time off work to manage the situation. This reflects a massive loss in productivity for our entire economy.

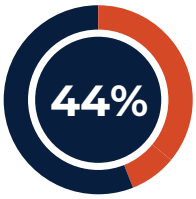
The implications for organisations

Australian organisations are too complacent about cyber security incidents.

Organisations need to better support their customers following a cyber security incident. The lack of support is eroding consumer trust, as respondents told us that doing the bare minimum causes an enormous loss of trust - just two per cent said they still trusted the organisation.

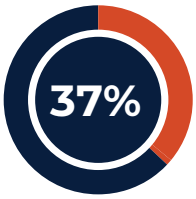
On the other hand, for organisations that acted quickly to provide clear, transparent information and clear guidance to help consumers protect themselves, there were significantly improved results in trust and reputation:

- 44 per cent of people say they would use the organisation again
- 40 per cent would trust the organisation
- More than one-third would recommend it to others (37%).



of people say they would use the organisation again

would trust the organisation



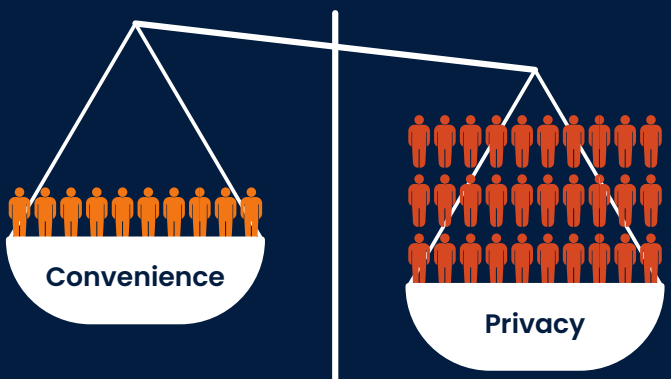
More than one-third would recommend it to others

As large scale cyber security incidents continue to impact thousands of Australians, consumers may increasingly forego convenience for privacy.

Three-quarters (75%) of Australians reported that the privacy of their personal data was more important than the convenience of online services. While this is a leading indicator, this result has climbed from 63 per cent in January 2023.

This is bad news for organisations whose marketing functions are built on data collection and analysis, and offer no real consumer benefit in return for harvesting, storing and on-selling their private data.

In the wake of many highly-publicised cyber incidents, it's important for organisations to think carefully about the way they collect, store and profit from their customers' data.



75%

of Australians reported that the privacy of their personal data was more important than the convenience of online services

What can organisations do?

There are three key actions organisations can take to build customer trust and protect their reputation in the event of a cyber security incident:

1. Pull the trigger sooner and tell customers about cyber security incidents faster.

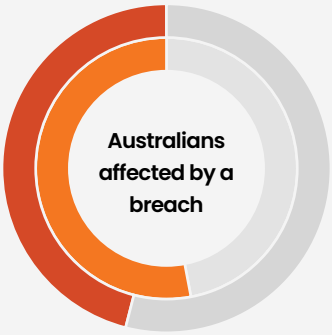
The OAIC allows organisations 30 days to assess whether a cyber security incident is likely to result in serious harm, but customers expect to be told much sooner.

While half of respondents (53%) agreed that organisations provided them with the information they needed about the incident, only 46 per cent of people impacted felt they were provided with timely information and support.

Organisations that seek to maintain trust with their customers must consider acting faster to provide as much clear information as possible about the incident, if they're serious about protecting their reputation.

53%
agreed that organisations provided them with the information they needed

46%
felt they were provided with timely information and support



2. Communicate more comprehensively.

If organisations only communicate the fact that a cyber security incident has occurred to affected consumers, they're only doing half the job, particularly if the incident is publicised and non-affected consumers will be aware of it.

It's easy for organisations to focus on the legal and technological issues in the wake of an incident, but they can't forget to address the equally crucial brand and communications issues that arise.

Our research identified six recommended communications actions organisations should take to properly respond to a cyber security incident:

1. **Do everything you can to protect customers from harm**
2. **Provide timely information and update it as required**
3. **Provide transparent information**
4. **Provide all the necessary information**
5. **Provide accurate information**
6. **Provide clear steps that customers need to take to protect themselves.**

We asked respondents questions about organisations that take 5-6 of the key recommendations. Forty per cent said they would trust them in the future, 44 per cent said they would be more likely to purchase from the organisation again, and critically, 37 per cent said they were more likely to recommend the organisation to others.

When it comes to this crucial version of a net promoter score, just four per cent said they would recommend organisations that took none of these actions.

That is a catastrophic result for customer acquisition, on top of the enormous costs of a cyber security incident.

To truly arm against reputational damage, organisations need to do more than the bare minimum when communicating with impacted stakeholders.

3. Empathy and customer experience is the key to securing trust.

Aside from the initial frustration at being affected by a cyber security incident, consumers find them to be deeply stressful experiences, with considerable administrative burdens.

In addition to the emotional toll, consumers are also faced with a time-consuming nightmare. This includes procuring new identity documents and financial details, cancelling tax file numbers and waiting for new bank cards.

Nearly half (48%) of those impacted experienced emotional distress following a cyber security incident. In addition:

- One in 10 (9%) had to take time off work to handle the situation
- Almost one in three (30%) had to update their ID documents
- One in five (22%) had to update their financial details.

It's important for organisations to acknowledge the burden this places on their customers when formulating their response and communications.

Too many consumers are forced to take matters into their own hands after a cyber security incident. Almost one-quarter (23%) of respondents impacted by a cyber security incident said they had to contact the organisation to find out more about the incident or to deal with a problem that arose as a result of the incident.

If you're a consumer-facing business, it's important to remember that cyber security incidents happen to people. Is your planned approach to incident response consistent with the way you plan your overall customer or employee experience?

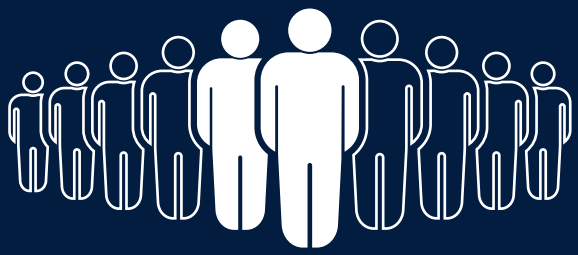
If not, you may be about to let down your customers at a critical time. Now is the time to consider how your "cyber incident customer experience" will look so you don't break that trust.

48%

of Australians experienced emotional distress following a cyber security incident

One in 10
had to take time off work to handle the situation

Three in 10
had to update their ID documents



One in five
had to update their financial details.

PORTER NOVELLI

About Porter Novelli

Porter Novelli is a Public Relations and Communications firm with extensive experience in cyber security incident response. We have worked with a range of clients across a variety of sectors and jurisdictions to prepare for and respond to sensitive and high-profile data breaches. We partner with legal and forensic IT teams, as well as insurers, to assist clients in navigating high-pressure cyber security incidents.

Quantum Market Research

About Quantum Market Research

Quantum Market Research is a full-service Social and Market Research agency that helps change-makers in business, government and philanthropy across a range of sectors make better decisions. Our work is grounded in a deep understanding of human behaviour, social sciences, advanced analytics and over 25 years of tracking culture change in Australia. The Quantum approach applies big picture thinking to every brief, no matter how targeted or unique, arming clients with the knowledge and understanding about people to drive insightful and meaningful decisions.