Beyond the Breach

Aligning Consumer and Business Expectations in Cyber Incident Response

August 2025

PORTER NOVELLI | Hall&Wilcox smarter law | Quantum Market Research

Legal Disclaimer

This cyber breach key findings report and associated presentations are current as at 27 August 2025. The contents do not constitute legal advice and are not intended to be (and must never be) used or relied on as a substitute for legal advice.

Before acting on any matter in this area, you should discuss your situation with a suitably qualified professional advisor. You should never delay seeking legal advice, disregard legal advice, or commence or discontinue any legal action because of the contents of this report.

PORTER NOVELLI | Quantum Market Research | Hall&Wilcox

Contents

04 Every Australian organisation will be impacted by a cyber security incident at some point, and the likelihood is only increasing

06 Privacy has never been more important to consumers

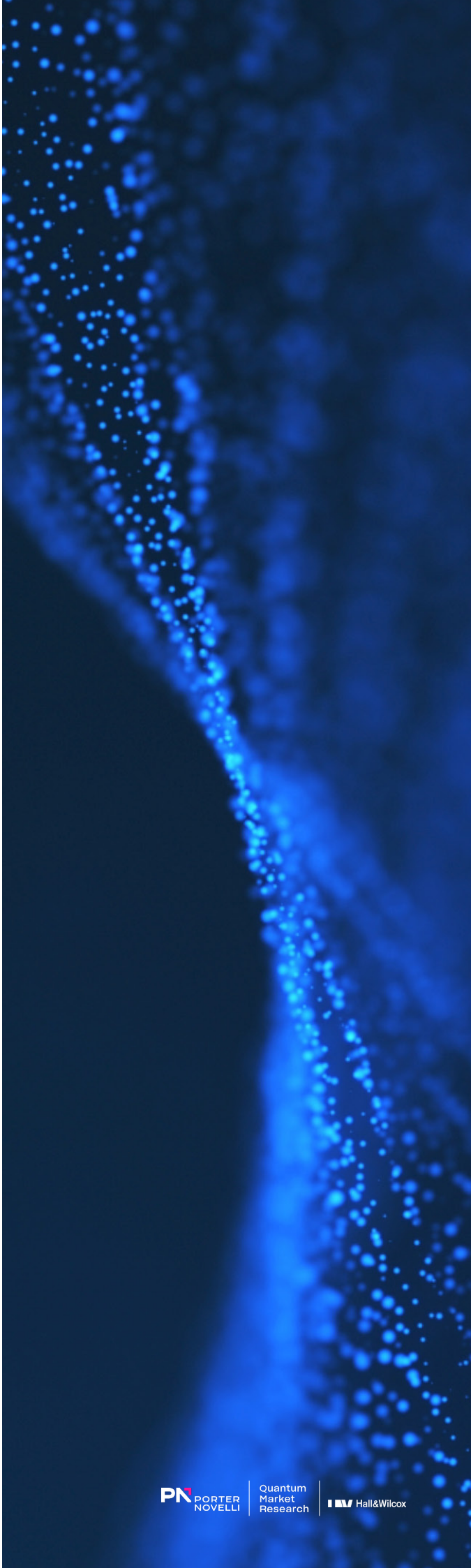
08 Financial data tops consumers' and business leaders' concerns in cyber incident

09 Australians remain distressed, even as concern about cybercrime fluctuates

10 Consumers demand faster speed of information

12 Organisations are not doing enough to protect customer trust

15 What can business leaders do?



PN PORTER NOVELLI | Quantum Market Research | Hall&Wilcox

Every Australian organisation will be impacted by a cyber security incident at some point, and the likelihood is only increasing

Cyber incidents are a growing reality for Australian business leaders and consumers. While several cyber security incidents have made headlines during the past two years, many people are not aware that there were more than 1,100 notifiable data breaches reported to the Office of the Australian Information Commissioner (OAIC) in 2024 alone. We suspect that many additional data breaches are not reported either because the organisations did not even know their security had been breached, were not aware of their legal obligations or chose not to notify, in breach of their legal obligations.

The 1,100 reported breaches is the highest annual total since the notifiable data breaches (NDB) scheme began in 2018, representing a 25 per cent increase from 893 notifications in 2023. These incidents affected millions of Australians.

As leading legal and communications firms advising on response and preparation for cyber incidents, Hall & Wilcox and Porter Novelli have worked on hundreds of these incidents in recent years.

Porter Novelli conducts regular research into best practices in cyber incident preparation and response, including our 2023 research into consumer expectations of organisations during an incident.

This year, Porter Novelli partnered with Hall & Wilcox and Quantum Market Research to conduct further research with a representative sample of Australians and a group of C-suite executive leaders and board directors. This research supports understanding of the impact of these incidents on both consumers and business leaders.

In 2024 there were 1,113 notifiable breaches, affecting millions of Australians

PORTER NOVELLI | Quantum Market Research | Hall&Wilcox

This study provides insights into two key areas:

1. **How consumer expectations have evolved over the past two years regarding the way organisations behave when they have suffered a cyber incident; and**

2. **The disconnects between consumer expectations and business leaders' views on what their obligations and priorities should be during a cyber incident.**

We are sharing these insights to help business leaders understand what consumers expect during a cyber incident, and how to more effectively support individuals impacted by a cyber incident.

Consumer expectations are not fixed – they are strongly shaped by news cycles, political pressure and lived experiences – but the need for empathy and transparency remains consistent over time.

Privacy has never been more important to consumers

Australians reveal that privacy trumps convenience in a way that could not have been predicted 10 years ago.

Three-quarters of Australians (75 per cent) care more about the privacy of their data than benefiting from the convenience of online technology. This is a 12-percentage point increase in the past two years.

This sentiment is echoed by business leaders, as three-quarters (75 per cent) agree their customers care more about privacy than online convenience.

Scepticism about the altruism of Big Tech has been growing since the Cambridge Analytica scandal in 2018 and the role played by social media in elections around the world. This scepticism has been supercharged by the combination of high-profile data breaches, further political activity of technology executives, and wariness of the utopian promises of AI developers.

As a result, nearly six in 10 (58 per cent) of Australians report they are more concerned about the security of their personal information online than they were five years ago.

The Australian privacy regulator, the Office of the Australian Information Commissioner (OAIC), is acutely aware of consumer expectations. In recent years, they have taken an increasingly assertive approach towards adoption by businesses of appropriate guardrails on data collection and processing practices, including the use of AI.

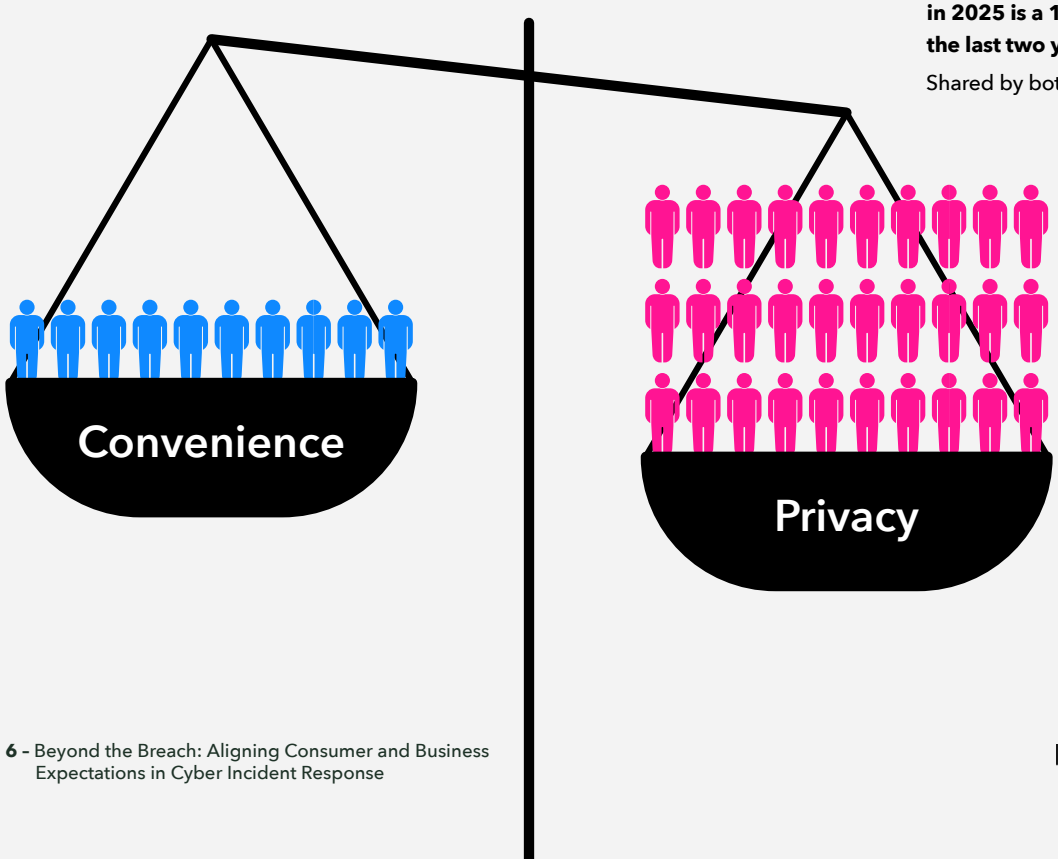
Businesses that do not meet regulatory expectations risk enforcement action.

This risk has been heightened in 2025, with the OAIC recently gaining expanded enforcement powers, including the ability to impose fines and commence legal proceedings for low to mid-range privacy interferences. Previously, regulatory enforcement proceedings by the OAIC required a 'serious or repeated' privacy interference, which may have discouraged them from taking strong action against all but the worst or most high-profile alleged offenders. We expect that these expanded penalties may result in an increased number and scope of data breach legal proceedings.

75%

in 2025 is a 12-percentage point increase in the last two years, up from 63 per cent in 2023.

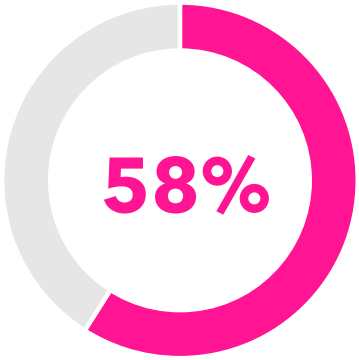
Shared by both consumers and business owners



As consumers grow more discerning about how they share their data, business leaders can't afford to underestimate the value their customers place on privacy. 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 consumers' personal information.

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

I am more concerned about the security of my personal information online than I was five years ago.



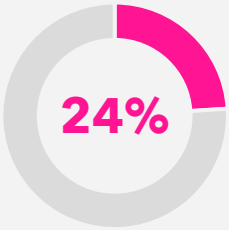
More than half of consumers agree

It's clear that most organisations are not living up to consumer expectations, which explains why almost half of consumers (48 per cent) report they are taking measures to protect their own personal information online.

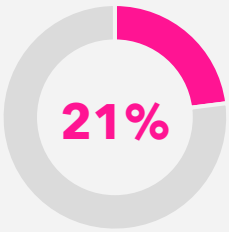
In the wake of highly publicised cyber incidents, it's important for organisations not only to think carefully about the way they collect, store and profit from their customers' data, but to communicate care for their customers' data.

Only 40 per cent of Australians agree that organisations can securely protect their personal information, and just half that number – 20 per cent – believe that organisations are actually doing enough to protect that information.

This has decreased significantly from two years ago, when 64 per cent of Australians believed organisations could securely protect their information, and 41 per cent thought organisations were doing enough. It is worth noting the latter has dropped more sharply – halving over just two years.



There is a 24-percentage point decrease in the number of Australians who agree that organisations can securely protect their information.



There is a 21-percentage point decrease in the number of Australians who believe organisations are actually doing enough.

An overtly strong approach to privacy can be a differentiator that will help organisations stand out in an increasingly sceptical market, particularly those whose stock-in-trade is data itself, such as a loyalty program, an e-commerce platform or online marketplace.

PORTER NOVELLI | Quantum Market Research | Hall&Wilcox

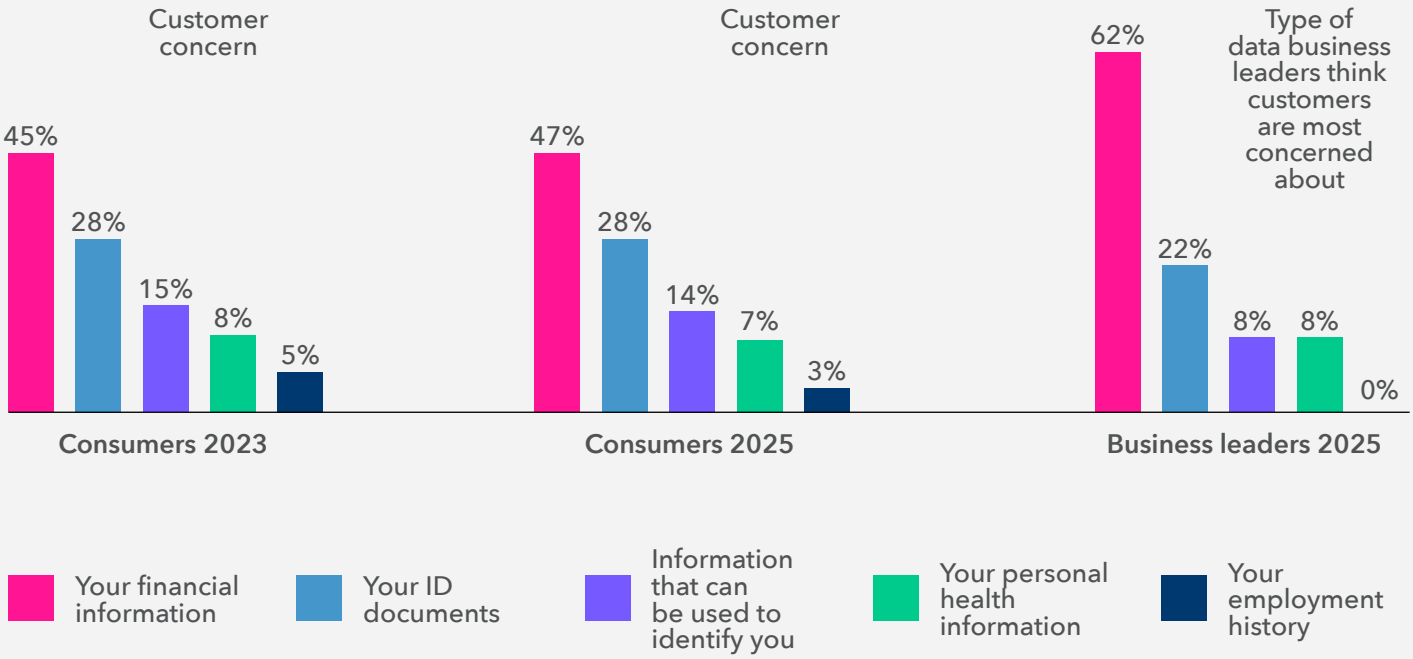
Financial data tops consumers' and business leaders' concerns in cyber incident

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

According to APRA, which recently introduced stronger security requirements for superannuation funds to keep members' money safe, Australia's financial institutions need to bolster cyber resilience. This reflects community concern. Our study found almost half of Australians (47 per cent) are more concerned about losing their financial information than any other information, which is consistent with 2023. More than six in 10 (62 per cent) of business leaders agree their customers are most concerned about their financial information.

This concern is warranted, according to data from the OAIC, which indicates that the financial sector ranked among the top three industries to report the most notifiable breaches in 2024.

As practitioners, we find that when an incident occurs, consumers tend to be equally concerned and upset about their medical, mental health, or employment data being stolen, but there is no doubt that loss of financial information and ID documents cause the greatest perception of risk and result in consumers having to spend significant amounts of time and resources to protect themselves.



Q. *Please rank the following types of information in terms of how concerned you / your customers would be if the following personal information was stolen.*

Australians remain distressed, even as concern about cybercrime fluctuates

Consumer and stakeholder expectations on the speed and transparency of response isn't fixed.

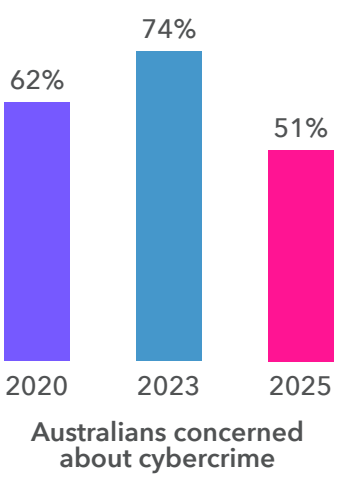
When asked how worried they are about cybercrime, Australians' concern peaked in 2023, with 74 per cent expressing significant concern, before dropping to 51 per cent by June 2025.

However, the emotional toll of a cyber incident remains unchanged, with 45 per cent of Australians who experienced a data breach reporting emotional distress in 2025, consistent with 48 per cent in 2023.

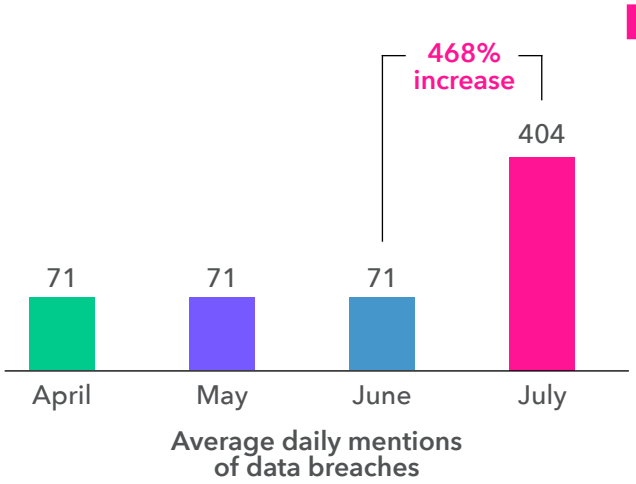
Our research shows that the level of concern among Australians remains highly variable, and is reactive to high-profile breaches, media coverage and political agendas.

When high-profile cyber incidents dominated news headlines in 2023, Australians reported heightened anxiety about cybercrime. By contrast, the weeks leading up to our June 2025 study contained a quieter news cycle, which may have contributed to the relatively lower number. However, just two weeks later, another massive cyber incident affecting millions of Australians made headlines again.

Daily mentions of "data breaches" in the news jumped from 71 per day in the three months leading up to our study, to more than 400 per day in the month following our study. We believe that if the survey was re-issued in July, we would have seen that concern number spike all over again.



Australians concerned about cybercrime

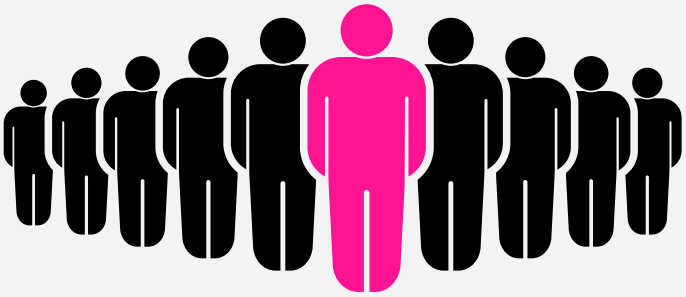


Average daily mentions of data breaches

Q. To what extent do you agree with the statement 'I am increasingly concerned about cybercrime?'

Despite the survey showing a drop in the number of consumers who expressed significant concern about cybercrime, the social and emotional impact of an incident doesn't change. One in 10 (10 per cent) people had to take time off work to manage the situation when they were impacted by a cyber incident in 2025, consistent with nine per cent in 2023. This reflects an ongoing loss in productivity for our entire economy.

Following recent legislative amendments, individuals may have the ability to bring proceedings directly against businesses who interfere with their privacy if they do so intentionally or recklessly. While this new law has not yet been tested by a court, we expect to see an increase in legal proceedings relating to data breaches.



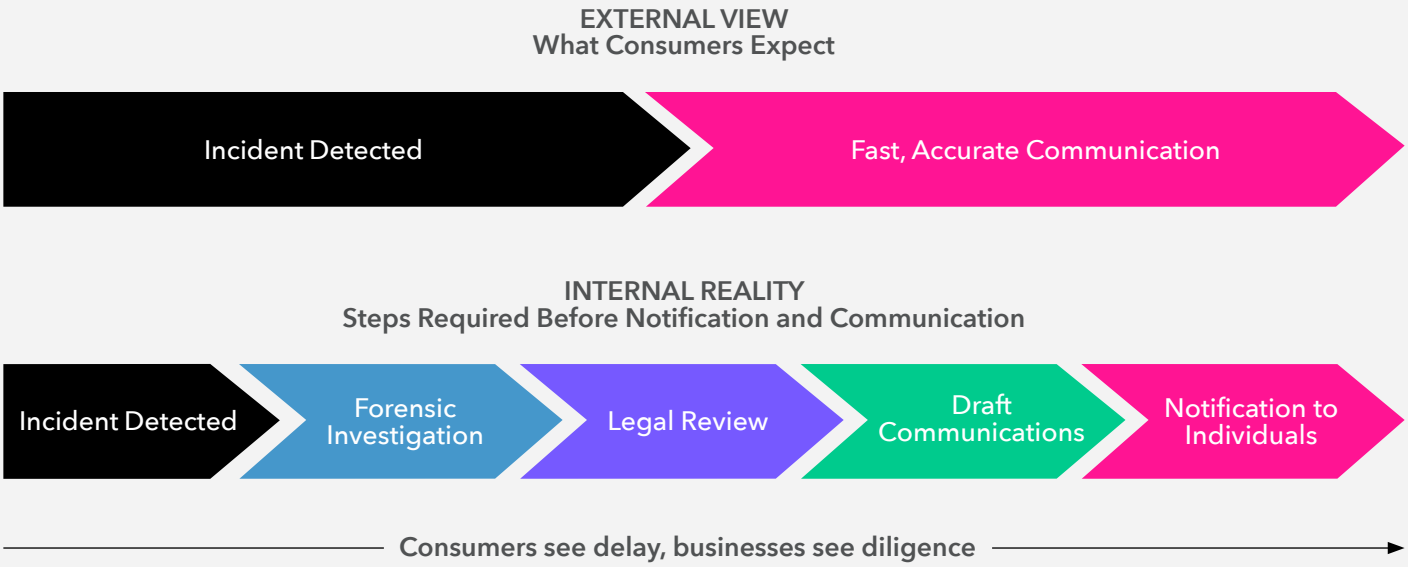
One in 10 (10%) had to take time off work due to a cyber security incident.

PN PORTER NOVELLI | Quantum Market Research | Hall&Wilcox smarter law

Consumers demand faster speed of information

Australians expect timely information, but this means different things in different situations.

"Fast enough" is not a fixed rule. Consumer/stakeholder expectations strongly depend on the sort of organisation you are, and the sort of spotlight that is on your organisation. Fewer than half of Australians (46 per cent) impacted by cyber incidents felt they were provided with timely information. However, the actual speed of response is very different to the speed at which a cyber incident unfolds.



Speed of resolution is more important to business leaders than it is to customers.

Where almost one third of Australians (31 per cent) call for timeliness, 28 per cent of business leaders think speed of resolution is as important as providing customers with transparent information.

And "speed" means different things to different stakeholders and organisations.

If an organisation is a household brand or critical infrastructure, stakeholders likely have higher expectations of fast, transparent communications than they do of a lesser-known or B2B brand.

Well-known organisations occupy a unique position of visibility and trust. They are also more "clickable" which makes a breach involving their organisation far more likely to drive media coverage, even if their involvement is tangential. At the same time, high-profile organisations (household brands, major government entities) and critical infrastructure (banks, airlines, telecommunications) may be forced to make an incident public before they have had time to investigate what has happened and what data has been impacted.

When an incident at a well-known brand becomes public, the expectation is near-instant response. Consumers assume household brands have more resources and therefore demand a higher standard of speed, clarity and accountability when something goes wrong.

By contrast, smaller businesses, B2B business or service providers may have more leeway. If the incident is unlikely to be public knowledge, they can take more time to analyse the data and tailor communications.

Speed of notification can create numerous legal risks, particularly if early communications turn out to be inaccurate.

This is what customers and stakeholders think is fast for different types of organisations

1 Day → **2 Weeks** →

Household brand or critical infrastructure

- Incident becomes public quickly
- Customers find out before forensics are complete
- Customers demand transparent, timely information

Lesser-known brand – MSP or SME

- Incident is unlikely to be made public
- Beneficial to take the time to analyse impacted data
- Communicate accurately with impacted individuals rather than alarm your entire customer base unnecessarily

Organisations are not doing enough to protect customer trust

Transparency is expected, not optional.

Our respondents told us organisations need to support their customers, members, employees or donors more effectively following a cyber security incident, which is consistent with the results in 2023.

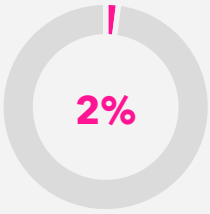
One hundred per cent of business leaders agree that their customers expect their organisation to provide transparent information in a cyber incident, yet only half (50 per cent) agree business leaders should go beyond basic legal requirements.

Recognition without action is risky for business leaders, as a lack of support continues to erode consumer trust.

Organisations that do the bare minimum following a cyber incident are still only trusted by two per cent of Australians.

CONSUMERS:

Thinking about the most recent data breach where you were notified of lost information or documents, are you more or less likely to trust the company involved?

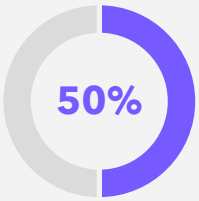


Companies who do the bare minimum are still only trusted by two per cent of Australians, consistent with 2023.

BUSINESS LEADERS:

If your company was impacted by a data breach and you were legally required to notify impacted individuals, to what extent do you agree with the following statements?

Business leaders agree that customers expect their company to provide transparent information.



Half agree they should go beyond basic legal obligations.

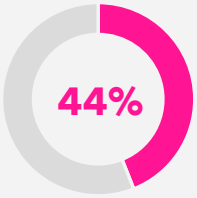
On the other hand, for organisations that acted quickly to provide clear, transparent information and guidance to help consumers protect themselves, there were improved results in trust and reputation:

- 25 per cent would purchase from the organisation again.
- 23 per cent would recommend the organisation to others.
- 23 per cent would trust the organisation.

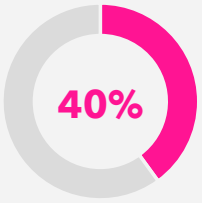
These are significant improvements compared to those where organisations are seen to have done the bare minimum, but, overall, it appears that Australian organisations remain too complacent about cyber security incidents.

In 2023, a higher percentage of consumers said they would re-engage with the organisation involved, which indicates that organisational response to cyber security incidents is eroding customer trust over time.

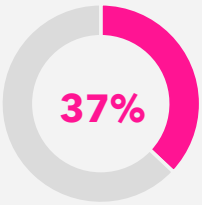
2023



Of people say they would use the organisation again.

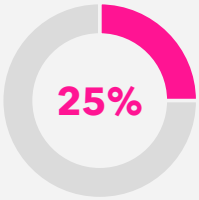


Would trust the organisation.

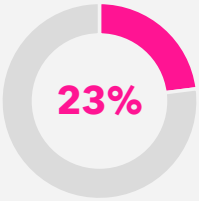


More than one-third would recommend it to others.

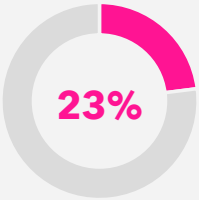
2025



Would purchase from the organisation again.



Would trust the organisation.



Would recommend the organisation to others.

PORTER NOVELLI | Quantum Market Research | Hall&Wilcox

Trust is critical, especially for older and younger Australians.

One third (33 per cent) of Australians are frustrated by the lack of timely information that was provided to them when they were impacted by a cyber incident over the past 12 months, and 27 per cent report the organisation didn't provide guidance on how they could protect themselves.

This is especially true for younger Australians. Forty-three per cent of people aged between 18 and 29 say companies failed to provide clear guidance on how to protect their personal information in the wake of a cyber incident.

People aged 65 and over are less likely to report frustration, but when they do, 56 per cent reveal organisations didn't protect them from harm – the highest across all age groups.

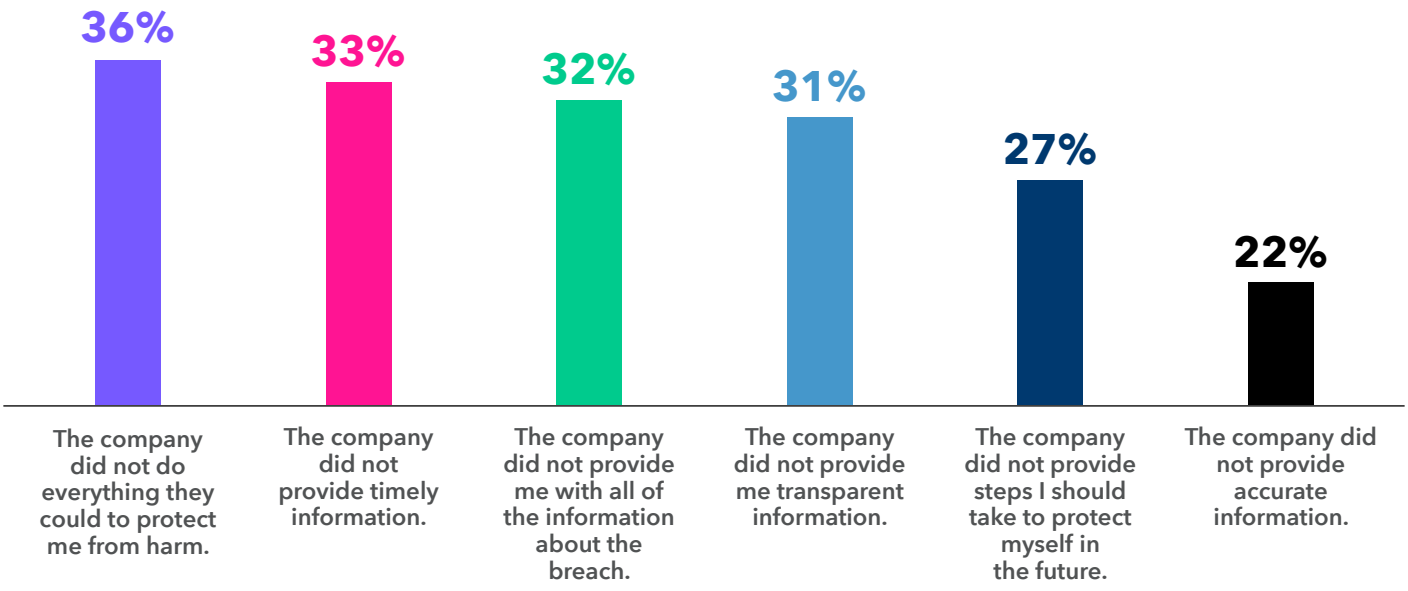
In contrast, almost two thirds of business leaders (62 per cent) feel they're doing enough to protect customers' personal information. This highlights a gap between business leaders' confidence and customer experience.

When a cyber incident occurs, older consumers feel especially vulnerable, and younger consumers expect proactive, educational responses.

Business leaders need to close the gap between acknowledgement and action, or they risk eroding customer trust and loyalty.

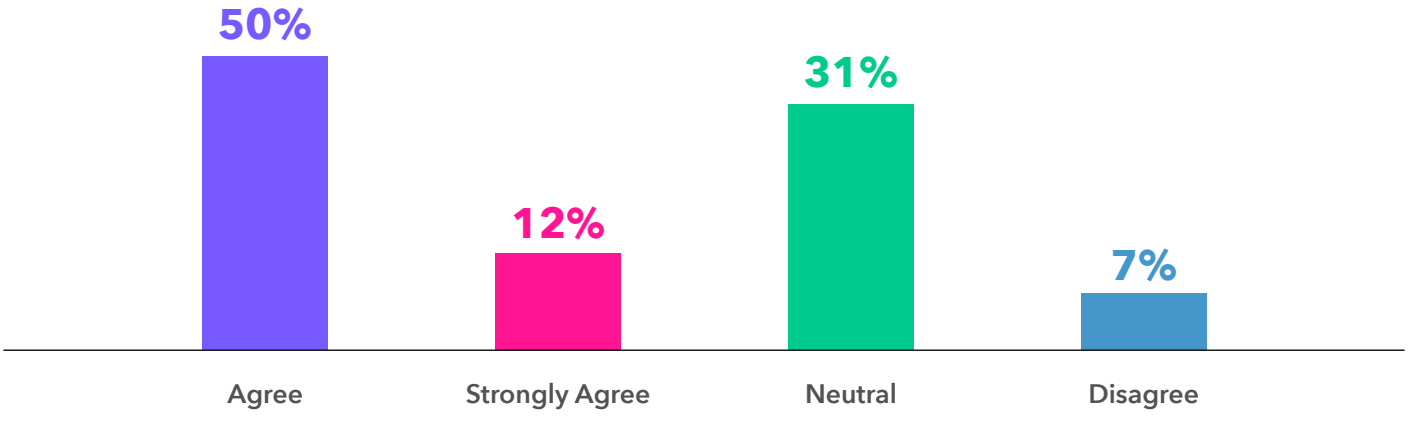
CONSUMERS:

Thinking about the cyber incident that left you feeling the most frustrated by the organisations' response, what did they not do to make you feel this way?



BUSINESS LEADERS:

To what extent do you agree with the statement 'my company is doing enough to protect my customers' personal information?'



What can business leaders do?

There are three key actions business leaders can take to build customer trust and close the gap between their priorities and consumer expectations in the event of a cyber security incident.

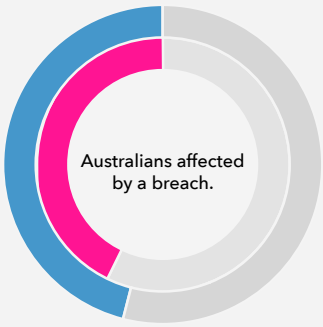
1. Communicate faster and smarter – in line with their stakeholders' expectations

Australians expect to be told quickly if their data has been compromised. While the NDB scheme allows 30 days to undertake an assessment of a suspected eligible data breach to determine whether notification is required, Australians expect to be told much sooner. Over the past two years, only 46 per cent of impacted consumers say they received timely information, and frustration is highest when organisations delay or provide what customers perceive as vague updates.

Organisations also need to understand their particular group of stakeholders and what their "customer cyber experience" is during a breach. A household name brand that may be called out quickly if there is an incident must have a materially different risk appetite and level of preparedness compared with a relatively unknown brand or entity.

48%
agree the organisation provided them with the information they needed

46%
felt they were provided with timely information and support



Q. Thinking about the most recent data breach where you were notified of lost information or documents, how did you feel?

2. Go beyond legal requirements with transparency

Consumers consistently lose trust when organisations simply meet legal obligations. As trust levels continue to drop, organisations can differentiate and protect against reputational damage by "going above and beyond" when communicating with impacted stakeholders. This can mean bringing in independent expertise to review the incident and provide recommendations for improvement, offering services for impacted individuals when appropriate, or being able to stand up virtual contact centres to quickly, accurately and transparently handle the flood of inbound enquiries.

3. Prioritise empathy

Consumers want to feel supported when their information is compromised and both studies from 2023 and 2025 highlight the emotional toll of a cyber incident. Almost half (45 per cent in 2023, 48 per cent in 2025) of Australians report distress, with one in 10 needing time off work to remediate the issue, such as replacing IDs or financial details.

Organisations that acknowledge this burden by providing accessible help, and frame their response around people rather than systems, see stronger trust and loyalty outcomes. In 2023, organisations that took multiple proactive steps were far more likely to be trusted and recommended by consumers, a pattern that remains in 2025.

Overall, organisations are best placed when they understand their stakeholders' expectations and are prepared to act and communicate in line with their publicly stated values. Cyber incidents are no different, and organisations who both prepare and test their incident response procedures will be better placed to meet consumer expectations when (not if) the real thing happens.

Many brands roll out the red carpet when consumers are looking to spend money with them, only to shut up shop when they've had an incident and consumers want answers to important questions. Nothing kills reputation and trust more effectively. Solid preparation will help every organisation meet and exceed its stakeholders' expectations. And when that happens, a crisis becomes an opportunity to prove to customers, members, donors or employees that you are worthy of their trust.

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.

Hall & Wilcox

Hall & Wilcox is a leading Australian law firm, delivering outstanding legal services to corporate, public sector and private clients, both Australian-based and those offshore doing business in Australia. Our purpose is to enable our clients, our people and our communities to thrive. We're renowned for our Smarter Law approach. As a firm, we possess one of the largest and most experienced legal teams in Australia dedicated to assisting clients respond to cyber incident and data breaches. We work with clients across sectors who lead, challenge and reshape their own industries.

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.