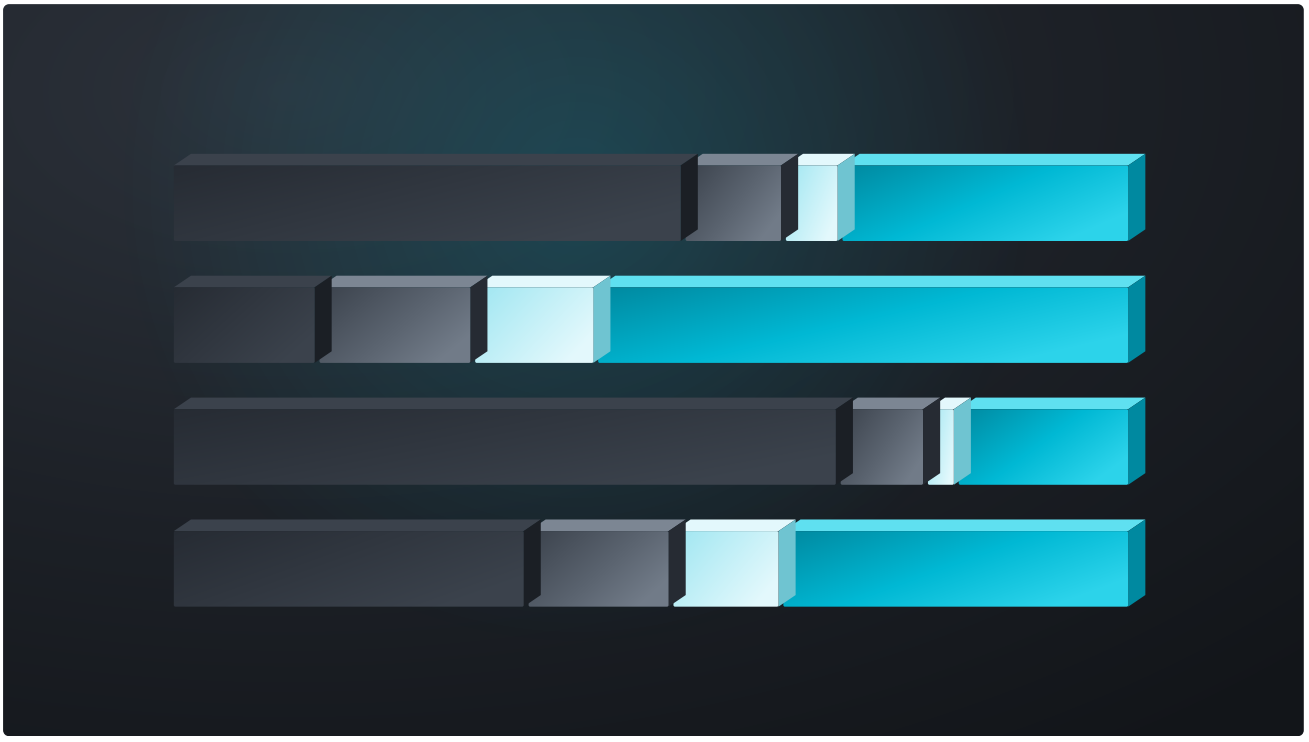
Black Shard

RESEARCH REPORT

How long Australian organisations took to find and report a breach, July to December 2025

In the second half of 2025, over half of the malicious breaches reported to the OAIC with a known time were found within ten days, and over half took more than 30 days to notify. The time is lost between finding the breach and deciding what it is, and a rehearsed assessment shortens that delay.



Entity	Black Shard Pty Ltd · ABN 66 696 910 773
Document ID	BS-RPT-11
Classification	Public
Version	1.3
First published	28 July 2026
This edition	16 November 2026
Figures	OAIC data of 1 Jul to 31 Dec 2025, read 28 Jul 2026

Executive summary

Australian organisations and agencies made 670 data breach notifications to the OAIC from 1 July to 31 December 2025. Malicious or criminal attacks accounted for 405 of the 670 notifications, human error for 194 and system faults for 35; the remaining 36 were recorded as other or currently unknown.

Malicious or criminal attacks took more than 30 days to notify the OAIC in 213 of the 382 cases with a known time, 56 per cent, and more than 30 days to identify in 113 of 373, 30 per cent. Of the 192 human error breaches with a known time to notify, 71 were notified within 10 days, 37 per cent, 29 took 11 to 20 days, 22 took 21 to 30 days and 70 took more than 30 days, 36 per cent.

An entity that suspects an eligible data breach has 30 days to assess it, then must notify the OAIC and the people affected as soon as practicable. The OAIC counts the time to notify from the day the organisation became aware of the breach, so a notification after more than 30 days has run past the window the Act allows for the assessment. In the half year, that was the outcome for most malicious attacks and for more than a third of the breaches caused by error.

The figures separate two problems that are usually treated as one. Finding the breach was the quicker half: most of those with a known time were known within ten days of happening. Working out what was taken, deciding whether the harm is likely to be serious, and getting the notice out was the slower half, and it is the half a firm controls. A firm that has decided in advance who makes the call, what facts they need and where those facts are kept finishes the assessment in days. A firm deciding those things during the breach spends its 30 days on them.

- Name the person who decides whether a breach is likely to cause serious harm, and the deputy who decides when they are away.
- Keep the sign-in, mailbox and file access logs that answer what was reached, for longer than an attacker stays unnoticed.
- Run the assessment as a drill once a year against a made-up breach, and time it.

Method

Every figure comes from the dataset the Office of the Australian Information Commissioner published on data.gov.au for the notifications it received from 1 July to 31 December 2025, which its release of 6 July 2026 links. We read every table on 28 July 2026 and print each count as the OAIC states it.

The OAIC reports the days taken to identify a breach and the days taken to notify it in four bands: 10 days or fewer, 11 to 20 days, 21 to 30 days and more than 30 days. Time to identify counts the days from the breach occurring to the organisation becoming aware of it. Time to notify counts the days from awareness to the notification reaching the OAIC. The OAIC leaves out notifications whose dates fall outside the range, so the time tables add to fewer than the half year’s total, and every percentage is of the notifications with a known time, rounded to a whole number.

The scheme covers the agencies and organisations the Privacy Act binds. The Privacy Act’s small business line sits at A$3 million in annual turnover, and a business that provides a health service and holds health information is covered whatever its turnover. A breach at a business under the turnover line is usually outside the count, so the figures understate what happens to the smallest firms, and say nothing about how quickly they find out.

The assessment drill

When the clock starts. The 30 days begin when someone in the organisation has reasonable grounds to suspect an eligible breach: the moment a mailbox rule is found, a supplier rings, or a laptop is reported missing. The clock does not wait for the investigation to finish or for the facts to be certain. A firm that treats the first report as the start, and writes the date down, knows where it stands on every later day.

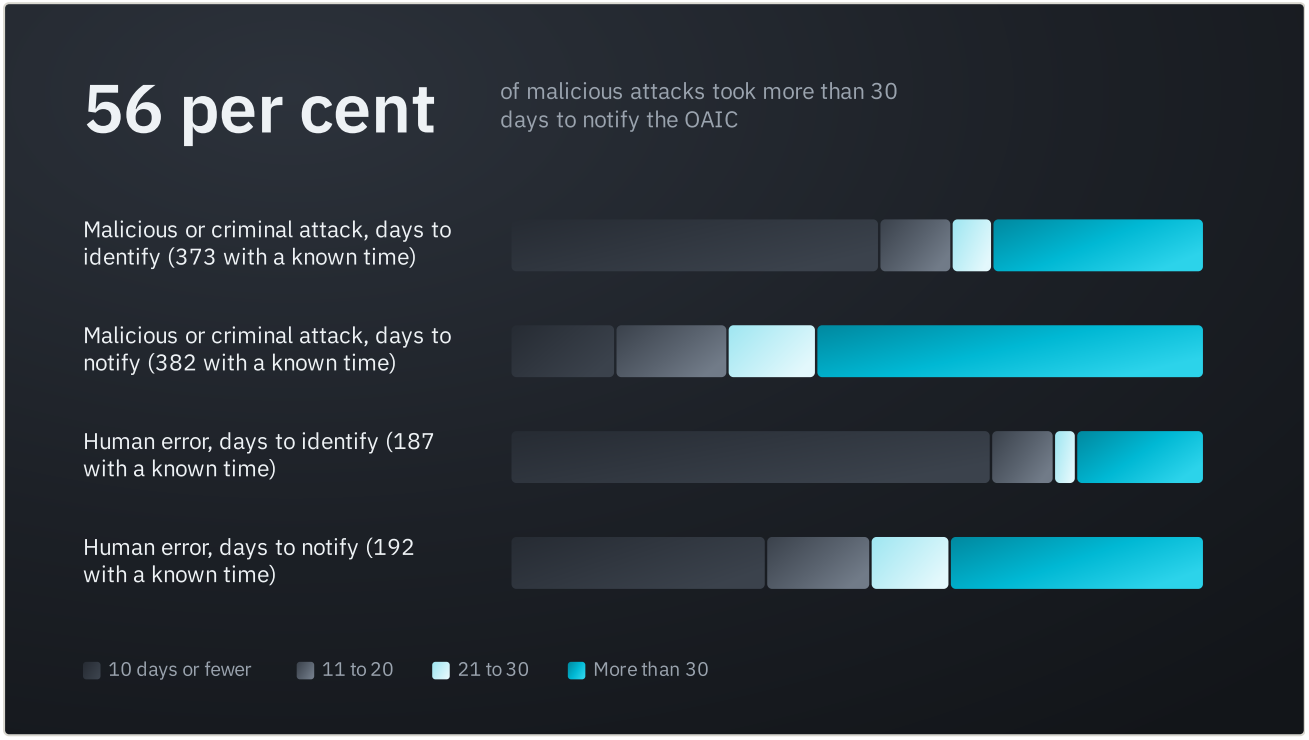
Who decides. One named person decides whether the breach is likely to cause serious harm to the people whose information was involved, with a deputy for the days they cannot be reached. The investigators report facts to that person; the decision stays with them whatever the investigation finds. In a small firm the decider is usually a director, and the drill is the first time most directors learn the test they will be applying.

What evidence. The assessment needs four facts: what information was involved, whose it was, who had access to it and for how long, and whether it was protected or has since been recovered. The first two come from the system that held the data. The third comes from sign-in logs, mailbox audit logs and the file access trail, and it is the fact most firms cannot establish, because the logs were never turned on or were kept for less time than the attacker spent inside. The fourth is a judgement on the first three.

How it ends. The assessment ends with a dated decision: the breach is notifiable and the notice to the OAIC and the notices to the people affected go the same day, or serious harm is unlikely and the reasons are kept with the file. Notices drafted in advance, with the facts left blank, turn the last step from a day of writing into an hour of filling in.

Found within days, reported after the window

DAYS TO IDENTIFY AND DAYS TO NOTIFY, BY SOURCE OF BREACH



Over half of malicious attacks were identified within 10 days, and over half took more than 30 days to notify the OAIC. Source: OAIC Notifiable Data Breaches dataset for 1 July to 31 December 2025, published on data.gov.au 29 June 2026.

Of the 373 malicious or criminal attacks with a known time to identify, 199 were identified within 10 days, 53 per cent, 39 took 11 to 20 days, 22 took 21 to 30 days and 113 took more than 30 days. Of the 382 malicious or

criminal attacks with a known time to notify, 58 were notified within 10 days, 15 per cent, 62 took 11 to 20 days, 49 took 21 to 30 days and 213 took more than 30 days.

Read together, the two rows describe a different problem from the one most firms prepare for. Detection was the faster half: over half of the attacks with a known time were known within ten days of occurring, and that share includes the ransomware cases that announce themselves. The slower half is everything after someone knows, and in 56 per cent of attacks it ran past the 30 days the Act allows. The breach was in hand long before the decision was.

Of the 187 human error breaches with a known time to identify, 130 were identified within 10 days, 70 per cent, 17 took 11 to 20 days, 6 took 21 to 30 days and 34 took more than 30 days, 18 per cent. Of the 192 human error breaches with a known time to notify, 71 were notified within 10 days, 37 per cent, 29 took 11 to 20 days, 22 took 21 to 30 days and 70 took more than 30 days, 36 per cent.

A wrong recipient or an open file share is usually found the day it happens, and the facts of what went where are known the same day, so the assessment should be short. Even so, more than a third of those breaches took more than 30 days to reach the OAIC. The delay is organisational: the breach sits with the person who made it until someone decides it is theirs to escalate, and the firm has never said whose it is.

For a small firm the lesson is the order of the work. Detection improves with tooling bought over years. The assessment improves in an afternoon, with a named decider, four facts written on one page, and two notices drafted in advance.

Where the half year's breaches came from

Malicious or criminal attacks accounted for 405 of the 670 notifications, human error for 194 and system faults for 35; the remaining 36 were recorded as other or currently unknown. The count ran at 117 in July, 99 in August, 116 in September, 122 in October, 99 in November and 117 in December.

Of the 405 malicious or criminal attacks, 253 were cyber incidents, 88 were social engineering or impersonation, 34 were a rogue employee or insider and 30 were theft of documents or a data storage device. A cyber incident in the OAIC's terms is the stolen credential, the phishing page, the ransomware and the exposed service. Social engineering is the call or the email that persuades a person to hand over access or change a payment, and it reached the OAIC as a breach in its own right in roughly one attack in five.

Of the 194 human error breaches, 66 were personal information emailed to the wrong recipient and 59 were an unintended release or publication. Both come from a person sending or publishing without a check, and both are reduced by the same two measures: fewer people able to send or publish personal information in bulk, and a check on what leaves the business before it goes.

The count was level across the six months, with no season in which a firm could expect a pause.

Agencies, health, and the people affected

Australian Government agencies took more than 30 days to notify in 43 of the 50 notifications with a known time, 86 per cent, and more than 30 days to identify the breach in 35 of 50. Agencies hold the most information and have the most people to consult before a notice goes out, and the count shows what that consultation costs in days. A supplier that holds an agency's information is inside that assessment from the day either party suspects a breach, and the agency will want the supplier's facts long before its own 30 days are up.

Health service providers made 128 notifications, the most of any sector, 64 from malicious or criminal attacks and 51 from human error. Health service providers identified 86 of the 117 breaches with a known time within 10 days, 74 per cent, and notified 43 of 124 within 10 days, 35 per cent. Health found and reported its breaches faster than finance, the associations and government, which fits a sector whose breaches are often found by the practitioner who caused them and whose duty to notify reaches every practice whatever its size.

More than 30 days to notify was the largest band in finance, 43 of 80, and in business and professional associations, 37 of 68; in health it was 41 of 124 and in personal services 15 of 43. Finance and the associations were closer to the government pattern than to health: breaches found by an outside party, assessed by a committee, and notified when the committee was satisfied.

One person was affected in 161 of the 670 breaches, the number affected was unknown in 18, and 4 breaches affected more than 1,000,000 people. Most breaches are small, and the assessment for a breach that reaches one person is the same assessment as for one that reaches a million. A firm that can run it quickly for the small breach is ready for the large one.

Contact information was involved in 537 of the 670 breaches, identity information in 386, financial details in 253, health information in 228 and tax file numbers in 151. Contact details on their own rarely meet the serious harm test; identity documents, financial details and health information usually do, and tax file numbers always warrant the question. The kind of information involved is the first of the four facts, and the quickest to establish if the firm already knows which systems hold which kind.

What to do

The drill below takes an afternoon. Run it against a made-up breach, a mailbox taken over for three weeks, and time each step. Where a step takes longer than a day, that is where the 30 days will go.

1. Write down who decides whether a breach is likely to cause serious harm, and who decides when they are away. Give both the OAIC's test on one page.
2. Write down what starts the clock: any report of a suspected breach, from anyone, logged with its date and hour.
3. List the systems that hold personal, health, financial and identity information, and the person who can pull an export from each one within a day.
4. Confirm that sign-in logs, mailbox audit logs and file access logs are on, and that they are kept for months: three in ten malicious breaches took more than 30 days to find, and the logs must still cover the day the attacker arrived.
5. Draft the notice to the OAIC and the notice to affected people now, with the facts left blank, and keep them where the decider can reach them without the IT provider.
6. Agree with each supplier that holds your clients' information how quickly it will tell you about a breach, and put the number of days in the contract.
7. Set the standard for your own firm: a decision within ten days of the first report, and the notices the same day as the decision.
8. Run the drill again when the decider changes, and once a year regardless.

Our free breach notification helper walks the serious harm assessment in the browser, with nothing sent to us. A firm that wants the drill run for it can engage us for breach readiness: we run the exercise with the directors, write the decision roles and the two notices, check that the logs answer the four facts, and leave a plan dated to the Act's

windows. When a breach is live, our breach remediation team contains it, establishes what was reached and supports the assessment and the notices.

Our record

Black Shard builds and defends the systems Australian organisations run on.

The record is as held at 16 November 2026, the date this edition was revised.

- SMB1001:2026 Gold, issued by CyberCert, valid 16 Jun 2026 to 17 Jun 2027.
- Essential Eight Maturity Level 3, assessed September 2026.
- Prequalified supplier to Queensland councils under Local Buy arrangement LB308, ICT Solutions, Products, Services and New Technologies.
- Prequalified supplier under the NSW Government ICT Services Scheme (SCM0020).
- Holder of Victorian Fair Jobs Code pre-assessment certificate FJC-261023-11119, required for Victorian Government threshold and high-value procurement.
- Approved supplier on the Tasmanian Government Technology Services List (TSL) for Application Development Services, Operational Technical Services and Cyber Security.
- Our CISO holds the Exemplar Global ISO/IEC 27001:2022 Lead Auditor credential.
- Professional indemnity, public liability, cyber and workers' compensation insurance, all current.
- More than 65,000 tests across our repositories, counted on 26 October 2026.
- More than 1,500 deploys and releases shipped since 27 April 2026.

> 24/7 incident line: 1800 370 270.

Sources

- OAIC, Notifiable Data Breaches (NDB) scheme: NDB Data 1 July 2025 to 31 Dec 2025, data.gov.au, resource created 29 June 2026: https://data.gov.au/data/dataset/5781dc17-2ad0-4dd1-bced-01c544943ce3/resource/e14c521b-0966-42cf-849b-0ef1214e8903/download/ndb-data-1-july-2025-to-31-dec-2025.xlsx
- OAIC, Data breach notifications increase to all-time high in 2025, new NDB stats show, 6 July 2026: https://www.oaic.gov.au/news/media-centre/data-breach-notifications-increase-to-all-time-high-in-2025,-new-ndb-stats-show
- OAIC, Notifiable Data Breaches scheme: https://www.oaic.gov.au/privacy/notifiable-data-breaches
- Privacy Act 1988 (Cth), Part IIIC