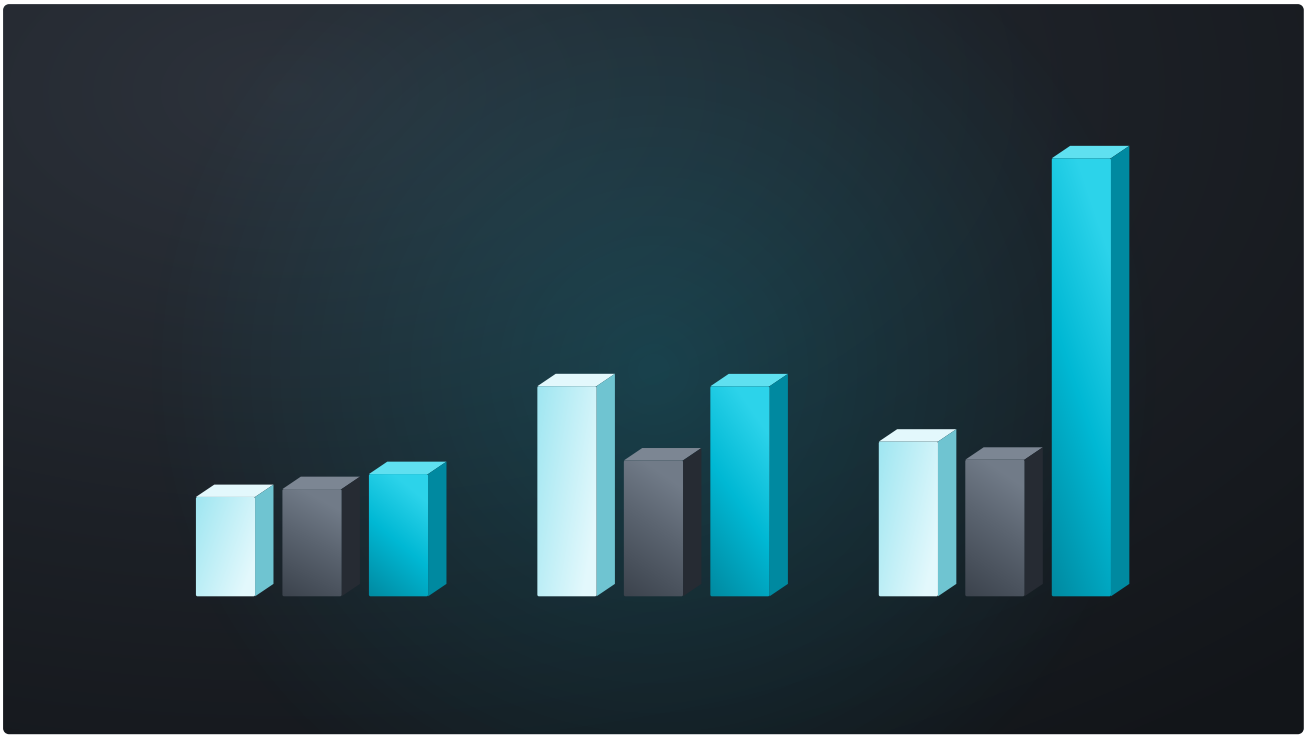
Black Shard

RESEARCH REPORT

What a cyber incident costs an Australian business

The Australian Signals Directorate puts a figure on what a cybercrime cost the business that reported it, by size of business, for the year to 30 June 2025. Three years of the figure show where each size band sits, and two of the three crimes businesses reported most are an attacker inside a mailbox.



Entity	Black Shard Pty Ltd · ABN 66 696 910 773
Document ID	BS-RPT-06
Classification	Public
Version	1.2
First published	17 February 2026
This edition	16 November 2026
Figures	ASD figures of 14 Oct 2025, read 17 Feb 2026

Executive summary

Businesses that reported a cybercrime to ReportCyber in the year to 30 June 2025 put its cost at $80,850 on average, up 50 per cent on the year before. A small business put the cost at $56,600 on average, up 14 per cent; the exact average was $45,965 in the year to June 2023, $49,615 in the year to June 2024 and $56,571 in the year to June 2025. A medium business put it at $97,200 on average, up 55 per cent; the exact average was $97,203 in the year to June 2023, $62,870 in the year to June 2024 and $97,166 in the year to June 2025.

ReportCyber received over 84,700 cybercrime reports in the year to 30 June 2025, down 3 per cent on the year before, one every 6 minutes. The three cybercrimes businesses reported most were email compromise with no financial loss, 19 per cent of business reports; business email compromise fraud with a financial loss, 15 per cent; and identity fraud, 11 per cent.

The averages are what the reporting business estimated at the time it lodged the report, so each is a floor. For a small firm the small-business figure is the cost of one bad week: a mailbox taken over, an invoice paid into the wrong account, or a laptop encrypted. The professional fees, the lost days and the customers who leave arrive after the report is lodged and are mostly outside it.

Two of the three crimes businesses reported most begin with an attacker inside a mailbox, and the third, identity fraud, is often fed from what was read there. The controls that stop them sit at the base of every Australian standard: phishing-resistant sign-in, a rule for changes to bank details, authenticated outbound mail, and systems that are patched and backed up.

- Find your firm’s size band in the ASD’s figures and treat the average as the floor of what one incident costs.
- Put phishing-resistant multi-factor authentication on every mailbox, and confirm every change to bank details by phone.
- Decide now who runs the first hour, who calls the bank and who reports to ReportCyber.

Method

Every figure comes from the web edition of the Annual Cyber Threat Report the Australian Signals Directorate published on 14 October 2025, which covers the year to 30 June 2025. We read the edition on 17 February 2026 and print each figure as the ASD states it: the rounded averages and the rises from its summary, and the exact averages by business size for each of the three years in the figure in which it charts cost by business size.

The cost is self-reported. The business that lodged the report to ReportCyber estimated its own loss at the time, and nobody audited the estimate. The ASD prints the average for small, medium and large businesses. Take the band your firm would report under and treat its average as a floor: an estimate made in the first days of an incident rarely counts the lost work, the professional fees and the customers who leave.

Large businesses made just over 12 per cent of the business reports, down 22 per cent on the year before. We print the large-business average with the ASD’s caveat and build nothing on it.

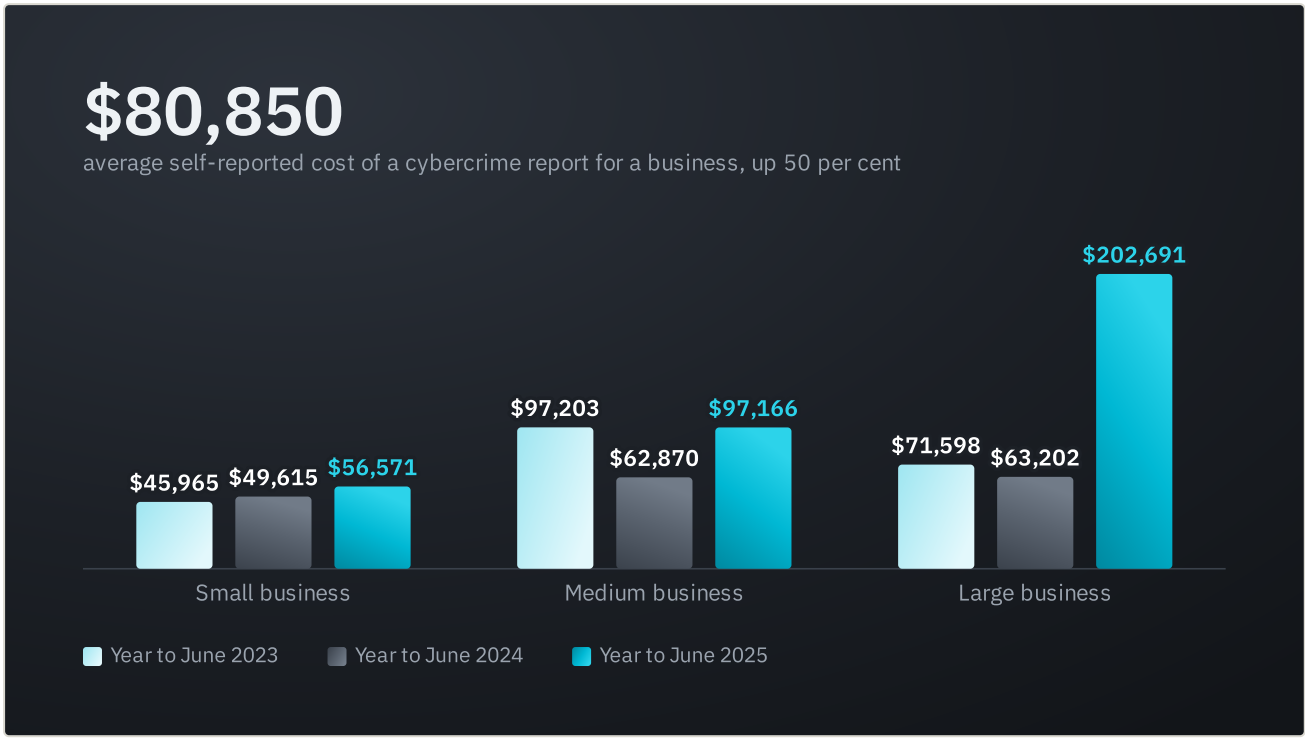
To read the figures against your own estate, take three numbers: the average for your band, the number of working days your business could run without its main systems, and the daily value of the work that would stop. The product of the last two is the part of the cost a reported average understates most. Our free incident cost estimator does the arithmetic in the browser from your own inputs and sends nothing to us, and the result is the number a board weighs the cost of controls against.

Each of the three crimes reported most has a control that stops it. Email compromise is stopped at sign-in by phishing-resistant multi-factor authentication, and caught early by an alert on new inbox rules and on sign-ins from places your staff do not work. Business email compromise fraud is stopped by a rule that every change to bank details is confirmed by phone on a number already held. Identity fraud is reduced by holding fewer identity documents for less time, and by authenticated outbound mail, so a message that forges your domain is rejected before it reaches a customer or your bank.

The cost of a report, by size of business

Businesses that reported a cybercrime to ReportCyber in the year to 30 June 2025 put its cost at $80,850 on average, up 50 per cent on the year before. A small business put the cost at $56,600 on average, up 14 per cent; the exact average was $45,965 in the year to June 2023, $49,615 in the year to June 2024 and $56,571 in the year to June 2025.

THE COST OF A CYBERCRIME REPORT, BY BUSINESS SIZE



Three years of the ASD's figure: the small-business average rose in each, the medium average returned to the level of two years before after a dip, and the ASD says the large-business rise may in part reflect the low number of reports from large businesses. Source: Australian Signals Directorate, Annual Cyber Threat Report 2024-2025, published 14 October 2025.

A medium business put it at $97,200 on average, up 55 per cent; the exact average was $97,203 in the year to June 2023, $62,870 in the year to June 2024 and $97,166 in the year to June 2025. A large business put it at $202,700 on average, up 219 per cent, the exact average being $71,598 in the year to June 2023, $63,202 in the year to June 2024 and $202,691 in the year to June 2025; the ASD says the rise may in part reflect the low number of reports from large businesses, which leaves the average open to outliers.

The medium-business average is the one to read closely, and over three years. It stood at the same level in the year to June 2023 as in the year to June 2025, with the dip between them, so the latest rise is a return to a level the figure had already reached, and that level is the one to plan on. A business of that size runs on the same cloud mail, the same practice or line-of-business systems and the same handful of administrators as a small one, and it holds

more of everything an attacker wants: more invoices in flight, more identity documents, more staff who can be impersonated. It rarely employs anyone whose job is security, so the response takes longer and costs more.

A small business pays less per incident and feels it more. The average lands in a week when the business also cannot invoice, take payments or answer its customers, and the owner is running the response. The figure to plan around is the band average plus the value of the days the business stands still.

The three crimes businesses report most

The three cybercrimes businesses reported most were email compromise with no financial loss, 19 per cent of business reports; business email compromise fraud with a financial loss, 15 per cent; and identity fraud, 11 per cent.

THE THREE CYBERCRIMES BUSINESSES REPORTED MOST



Two of the three are a compromised mailbox, and the third is often fed from one. Source: Australian Signals Directorate, Annual Cyber Threat Report 2024-2025, published 14 October 2025.

The first category is the mailbox taken over and read, before any money has moved. It is where the second category begins: a payment request altered, or a false invoice sent from an account the recipient trusts. Identity fraud, the third, is often downstream of both, fed by the scanned licence in a mailbox, the tax file number on a form and the customer list in a shared drive.

The three share a route in: a password, reused or phished, and a sign-in that accepted it. A firm that enforces phishing-resistant multi-factor authentication on every mailbox has closed the door on most of the first category and much of the second. The payment rule closes the rest of the second. Holding less identity information, for less time, shrinks the third.

The serious end

The ASD responded to over 1,200 cyber security incidents in the year to 30 June 2025, up 11 per cent, and 11 per cent of them included ransomware. The incidents the ASD responds to are the serious end: government, critical infrastructure and the organisations that call the hotline with an intrusion under way. Ransomware's share of them held steady, and a ransomware incident sits in a different order of cost from the averages above, because the business stops.

On 30 May 2025 the Australian Government introduced mandatory ransomware payment reporting for businesses with an annual turnover of $3 million or more. A firm over that line that pays a ransom now carries a reporting duty on top of the loss, and a firm under it still carries the loss. For both, the backup copy an attacker cannot reach, and a restore that has been timed, decide whether the ransom is ever a question.

What to do

Start with the three crimes the ASD's business reporters named most. For a firm with no security staff this is the order: each step stops a reported crime, and each can be read back from the system that enforces it.

1. Enforce phishing-resistant multi-factor authentication on every mailbox, including shared mailboxes and the owner's, and block the older sign-in methods that bypass it.
2. Write the payment rule and make it a habit: every new or changed bank account is confirmed by a phone call to a number already held, before any money moves.
3. Turn on alerts for new inbox rules, mail forwarding to outside addresses and sign-ins from places your staff do not work.
4. Publish SPF, DKIM and a DMARC policy that rejects, so mail that forges your domain is rejected by your customers' and your bank's mail servers.
5. Register the obvious near-matches of your domain, and tell your customers which address your invoices come from.
6. Patch the systems that face the internet on a short clock, and keep a backup copy that a compromised administrator cannot delete, with a restore that has been timed.
7. Hold identity documents only while you need them, in one place, with a deletion date.
8. Decide who runs the first hour of an incident, who calls the bank, who reports to ReportCyber and who decides whether a breach is notifiable, and write it on one page.
9. Put your own figures through an incident cost estimator and keep the result for the next conversation about what the controls cost.

We run incident response readiness as an engagement that starts with its scope, timeframe and price in writing: the first-hour plan, the payment rule, the alerts above turned on and tested, and a rehearsal with the people who would run it. The same basics are among the controls SMB1001 and the Essential Eight ask for, so a firm that wants a certificate or an assessed maturity level at the end of the work takes the uplift as one engagement. A firm with an incident under way goes to blackshard.com.au/breach.

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

- Australian Signals Directorate, Annual Cyber Threat Report 2024-2025, 14 October 2025: https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2024-2025
- Australian Signals Directorate, ReportCyber: https://www.cyber.gov.au/submit-a-report