



Australian Government
Australian Signals Directorate

cyber.gov.au

Annual Cyber Threat Report

2025–2026

Website

www.cyber.gov.au

Contact us

ASD's ACSC welcomes feedback to improve the services it provides to Australians. A feedback form can be found at cyber.gov.au.

Copyright

© Commonwealth of Australia 2026.

With the exception of the Coat of Arms, the entity's logo, third party content and where otherwise stated, all material presented in this publication is provided under a Creative Commons Attribution 4.0 Australian Licence. To the extent that copyright subsists in a third party, permission will be required by a third party to reuse the material.

Creative Commons Attribution 4.0 Australian Licence is a standard form licence agreement that allows you to copy, distribute, transmit and adapt this publication provided that you attribute the work.

The details of the relevant licence conditions are available on the Creative Commons website, as is the full Creative Commons legal code.

The Commonwealth's preference is that you attribute this publication (and any material sourced from it) using the following wording: © Commonwealth of Australia 2026, Australian Signals Directorate's Australian Cyber Security Centre, Annual Cyber Threat Report 2025–26.

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed at:

www.pmc.gov.au/government/commonwealth-coat-arms

Acknowledgement of Country

We acknowledge the Traditional Owners and Custodians of Country throughout Australia and their continuing connections to land, sea and communities. We pay our respects to them, their cultures and their Elders, past and present.



Australian Government
Australian Signals Directorate

cyber.gov.au

Annual **Cyber Threat** Report

2025–2026

Foreword

I am pleased to present the Annual Cyber Threat Report for 2025-26.

The world continues to face the most complex and challenging strategic circumstances since the Second World War. The rules-based international order, which has underpinned Australia's security and prosperity for decades, is in transition. Nations are increasingly contesting for influence, technological advantage and economic security. Cyber operations have become a central feature of this competition, offering adversaries a means to advance their objectives below the threshold of conventional conflict.

Over the past year, Australia continued to be targeted by cybercriminals and state-sponsored actors. These adversaries seek to compromise Australian government agencies, businesses and individuals to steal money and information, conduct espionage, undermine trust, and position themselves for future malicious activity. The line separating state-sponsored espionage from sabotage and cybercrime is becoming increasingly blurred.

Rapid advances in technology are further reshaping the threat environment. Artificial Intelligence (AI) is transforming economies, societies and national security capabilities at unprecedented speed. Since the second World War, no technology has carried greater potential to boost our sovereign capability, strengthen our national security and build our economic resilience. However, we must be clear-eyed with a threat-informed approach to advancing AI cyber capabilities with Australian sovereignty front and centre.

AI has been the defining force in the cyber threat landscape over the past year, allowing malicious actors to find vulnerabilities faster and exploit them at unprecedented scale, speed and sophistication. In recent weeks, new threats have emerged from the unintended actions of AI agents and model testing.

The successful adoption of AI by Australia will depend on balancing its considerable benefits with a clear understanding of its risks. In June 2026, the Australian Signals Directorate (ASD) and its Five Eyes partners released joint guidance outlining practical measures to manage AI-related cyber security risks, while enabling organisations to harness the technology safely and securely.

As Australia's foreign signals intelligence and cyber security agency, ASD has a unique view of the evolving threat environment. This report draws on those insights to provide an updated assessment of the threats facing Australia today and the trends that will shape the future of all Australians. Understanding these developments is essential to strengthening Australia's cyber resilience and ensuring our nation is prepared for the challenges ahead.

The report highlights that Australians continue to be affected by cybercrime, ransomware and data breaches, often resulting in significant financial, operational and personal harm. Cybercriminals are becoming more adaptive in their tradecraft, increasingly exploiting trusted relationships and using social engineering techniques to manipulate individuals and organisations into granting access to sensitive systems and information.

The cyber threat environment requires a greater focus on network resilience. In 2025-26, the Australian Signals Directorate's (ASD) ACSC responded to over 1,500 cyber security incidents, an increase of more than 20%, and notified entities of potential malicious activity more than 4,400 times, almost an 80% increase on the previous year.

The Australian Government's investment in ASD through Project REDSPICE continues to enhance its cyber capabilities and services to protect the nation. From providing insight into the tactics of malicious actors, to using offensive cyber operations to dismantle criminal infrastructure used to target Australians, ASD plays a vital role in supporting the nation's security and economic prosperity.

This report outlines the cyber threats we are facing and what we can do to strengthen our cyber resilience. We need all Australians to translate cyber awareness into practical action to improve our collective digital resilience.



The Hon Richard Marles MP

Deputy Prime Minister and Minister for Defence



Contents

About ASD's ACSC	viii
About the contributors	viii
Executive summary	1
Year in Review	3
What ASD's ACSC saw	3
What ASD's ACSC did	5
Timeline of key events and publications	9
Australian cyber threat landscape	16
Malicious use of AI	17
State-sponsored actors	21
Cybercriminals	23
Cyber in modern conflict	27
What malicious actors are targeting	29
Methods and tools	36
Resilience	42
What you can do	43
Report cyber security incidents to ASD's ACSC	51
Programs	53
Notes	57
Sources	57
Glossary	57
AI use disclaimer	57

About ASD's ACSC

The Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) is the Australian Government's technical authority on cyber security. Through the ACSC, ASD brings together capabilities to improve Australia's national cyber resilience. Its services include:

- providing the Australian Cyber Security Hotline, which is available 24 hours a day, 7 days a week, via **1300 CYBER1** (1300 292 371)
- providing technical advice and publishing alerts, advisories and notifications on significant cyber security threats
- monitoring cyber threats and sharing intelligence with partners, including through the Cyber Threat Intelligence Sharing platform (CTIS)
- helping Australian organisations respond to cyber security incidents
- providing exercises and uplift activities designed to enhance the cyber security resilience of Australian organisations
- supporting collaboration on cyber security issues between over 149,500 Australian organisations and individuals through ASD's ACSC Cyber Security Partnership Program.

Collaboration and partnerships are key to effective cyber security. ASD's ACSC thanks all the organisations that contributed to this report, including federal, state and territory government agencies, industry partners, and all who reported cyber security matters to ASD's ACSC.

About the contributors



The Australian Federal Police

The Australian Federal Police (AFP) is responsible for enforcing Commonwealth criminal law; contributing to combatting complex transnational, serious, and organised crime that impacts Australia's national security; and protecting Commonwealth interests from criminal activity in Australia and overseas. Operation Aquila leverages the complementary powers, capabilities and intelligence of ASD's ACSC and the AFP to disrupt the most serious cybercrime threats facing Australia. The AFP-led Joint Policing Cybercrime Coordination Centre brings together Australian law enforcement and key industry and international partners to inflict maximum impact on high volume, high harm cybercrime affecting the Australian community.



The Australian Security Intelligence Organisation

The Australian Security Intelligence Organisation (ASIO) is Australia's security intelligence service. It protects Australia and Australians from threats to their security, including terrorism, espionage, sabotage, and interference in Australia's affairs by foreign governments. ASIO's cyber program is focused on investigating and assessing the threat to Australia from malicious state-sponsored cyber activity. ASIO's contribution to ASD's ACSC includes intelligence collection, investigations and intelligence-led outreach to business and government partners.



Australian Government
Australian Institute of Criminology

The Australian Institute of Criminology

The Australian Institute of Criminology (AIC) is Australia's national research and knowledge centre on crime and justice. The AIC informs crime and justice policy and practice in Australia by undertaking, funding and disseminating policy-relevant research of national significance.



Australian Government
National Cyber Security Coordinator

The National Cyber Security Coordinator

The National Cyber Security Coordinator, supported by the National Office of Cyber Security, leads the coordination of national cyber security policy, responses to major cyber incidents, whole-of-government cyber incident preparedness efforts and the strengthening of Commonwealth cyber security capability. The Coordinator also oversees the implementation of the 2023–2030 Australian Cyber Security Strategy.



The National Anti-Scam Centre

The National Anti-Scam Centre, run by the ACCC, brings together experts from government, law enforcement and the private sector to disrupt scams before they reach consumers. The Centre is collectively committed to making Australia a harder target for scammers and reducing the financial and emotional harm caused by scams. The Centre does this through collecting quality scam reports through our Scamwatch service, collaboration (technology and intelligence sharing), disruption, awareness and protection.



The Australian Prudential Regulation Authority

The Australian Prudential Regulation Authority (APRA) is Australia's prudential regulator and is responsible for promoting the safety and stability of the financial system. APRA supervises banks, insurers and superannuation entities, setting prudential standards and overseeing resilience, risk management and financial soundness across the sector.



Australian Government
Department of Foreign Affairs and Trade

The Department of Foreign Affairs and Trade

The Department of Foreign Affairs and Trade (DFAT) promotes and protects Australia's international interests to support our security and prosperity. DFAT leads Australia's international engagement on cyber and critical technology across the Australian Government. This work is coordinated by Australia's Ambassador for Cyber Affairs and Critical Technology. DFAT is leading on the international elements of the 2023–2030 Australian Cyber Security Strategy, the development of which is being coordinated by the Department of Home Affairs.



Australian Government
Office of the Australian Information Commissioner

The Office of the Australian Information Commissioner

The Office of the Australian Information Commissioner (OAIC) regulates the compliance of Australian government agencies, organisations with an annual turnover of more than \$3 million and the compliance of some other organisations with the Privacy Act 1988 and other laws when handling personal information.



Australian Government
Department of Home Affairs

The Department of Home Affairs

The Department of Home Affairs is responsible for the leadership and central coordination of policy, programs and regulations relating to national security and resilience, law enforcement, migration and citizenship, multicultural affairs, and border management and security. The Department of Home Affairs leads the development of cyber security policy, including the implementation of the 2023–2030 Australian Cyber Security Strategy.



The Defence Intelligence Organisation

The Defence Intelligence Organisation co-leads the ACSC's cyber threat assessment team in partnership with ASD to provide the Australian Government with an all-source strategic, cyber threat intelligence assessment capability.

Executive summary

Technology is evolving at accelerated rates and continues to impact cyber security in both positive and negative ways. Throughout FY2025–26, Artificial Intelligence tools became more accessible, driven by a new generation of frontier AI models. These models have changed the game with speed and opportunity, but they have also generated significant uncertainty. The question is no longer whether organisations will face cyber threats, but how prepared they are to respond.

As AI tools become more accessible, malicious cyber actors require less effort to target Australian critical infrastructure (CI), governments, businesses, and individuals either for financial gain, espionage or to pre-position on systems for later disruption. Both state-sponsored actors and cybercriminals can use AI to identify vulnerabilities, develop exploits and launch attacks at greater scale than ever before.

To respond effectively to these new threats, organisations must radically speed up patching processes and adopt basic cyber security controls to remain resilient. Equally, the integration of AI tools into organisations' security operations can facilitate the early detection of vulnerabilities, enhance software quality, monitor for unusual behaviour and improve incident response times. The increasing integration of AI across the economy is expected to drive a greater focus on cyber security risk management practices – with the need to adapt to new threats, vulnerabilities and governance requirements associated with increasingly capable AI systems. The emergence of agentic AI, and the potential for rapid advances towards highly autonomous or recursively self-improving AI, may further accelerate the pace, scale and sophistication of cyber threats, requiring ongoing investment.

In FY2025–26, ASD's ACSC responded to more than 1,500 cyber security incidents, representing a 20% increase from the previous year and a 36% rise over the past five years. ASD's ACSC also notified entities more than 4,400 times of potentially malicious cyber activity – an increase of 80% over FY2024–25. This included over 2,200 individual notifications, and collective notifications issued to more than 2,100 entities.

State-sponsored cyber actors continued to target Australian organisations primarily to gain access to sensitive or non-public information. This activity extends beyond government networks, and includes critical infrastructure entities, private businesses and individuals. As the global security environment continues to deteriorate, state-sponsored cyber actors are increasingly seeking to pre-position within networks to enable future intelligence collection, disruption or access to higher-value targets at a time of their choosing. This trend is not confined to Australia and is evident in the context of multiple global conflicts currently underway. Cyber is a normalised and highly integrated feature of conventional warfare.

Australian individuals had personally identifiable information (PII) compromised in a growing number of global data breaches, and this data was held to ransom, sold or published online. AI has amplified the effectiveness of social engineering techniques, enabling malicious cyber actors to



more convincingly impersonate or manipulate Australian individuals and businesses for financial gain or access to networks. Compromised accounts and credentials also emerged as one of the most frequently reported incident categories across government, industry and CI sectors, reflecting the value malicious actors place on legitimate access to networks and systems. Implementing basic cyber security practices such as reviewing privacy settings, enabling passwordless authentication – such as multi-factor authentication (MFA) or passkeys – are essential to reducing the likelihood of becoming a victim of cybercrime.

In October 2026, ASD's ACSC released the Essentials series, evolving the Essential Eight into a modern, principles-based framework that provides prioritised, threat-informed cyber security guidance tailored to different technology environments. ASD's ACSC's Essentials series is a necessary reflection of advances in threats, availability of mitigation technologies and diversity of networks and operating systems.

In addition to modernising foundational frameworks, throughout FY2025–26, ASD's ACSC continued to amplify the importance for government, industry and CI entities of actioning priorities set out in our last year's report. This includes reducing legacy information technology (IT), implementing event logging, supply chain management, and preparing for post-quantum cryptography (PQC). Maintaining a focus on these priorities also ensures preparation for AI-enabled cyber threats. For example, the less legacy IT is exposed to the internet, the less attack surface opportunity there is for a malicious actor to compromise a network. In a similar vein, ceasing the use of traditional asymmetric cryptography by the end of 2030, or sooner, will ensure an organisation is at lower risk should AI speed up developments in quantum computing. AI capabilities have not introduced new cyber threats, but they have amplified and sped up existing ones, meaning action is now more critical than ever. Accordingly, these areas will remain a key focus for ASD's ACSC throughout FY2026–27.

It is critically important that organisations and individuals who observe suspicious cyber activity, incidents and vulnerabilities report to [cyber.gov.au](https://www.cyber.gov.au) or to the Australian Cyber Security Hotline **1300 CYBER1** (1300 292 371).



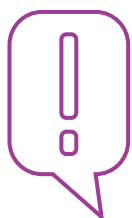
Year in Review

What ASD's ACSC saw



Answered over 37,500 calls to the Australian Cyber Security Hotline, down 12%.

- On average, 102 calls per day, a decrease from 116 calls per day.



Received over 82,000 cybercrime reports to ReportCyber.

- On average a report every 6 minutes, consistent with last year.



Individuals

Average self-reported cost of cybercrime per report for individuals remained consistent with last year (\$33,000).



Business

Average self-reported cost of cybercrime per report for businesses, up 16% overall (\$93,500).

- small business: \$55,400 (consistent with last year)
- medium business: \$141,300 (up 45%)
- large business: \$148,100 (down 27%).



Identity fraud remained the top reported cybercrime, down 18% from last year.



Publicly reported common vulnerabilities and exposures (CVEs) increased 30%.



Over 2,959,800 total users visited cyber.gov.au, generating nearly 6,281,700 views.



Over 262,800 downloads of our advice or guidance on cyber.gov.au.

Year in Review

What ASD's ACSC did



Responded to over 1,500 cyber security incidents, up 20% from last year.



Notified entities of potential malicious cyber activity more than 4,400 times, up almost 80%, to help prevent incidents before they occurred, including:

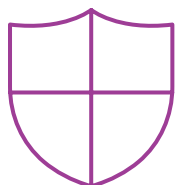
- Over 2,200 individual notifications, up 33%.
- Collective notifications to over 2,100 entities.



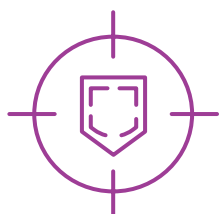
Identified 362 incidents following proactive notifications.



Responded to 139 ransomware incidents, consistent with last year.



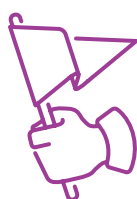
Australian Protective Domain Name System processed more than 220 billion queries and blocked customer access to over 564 million malicious domains.



Cyber Threat Intelligence Sharing (CTIS) grew by 22% to over 550 partners, and shared over 1 million indicators of compromise via the platform.



ASD's Cyber Security Partnership Program grew by 12% to over 149,500 partners.



Led 15 cyber security exercises, involving over 335 organisations.



Briefed board and executive leadership team representatives from 29% of the ASX100.

Year in Review

What ASD's ACSC did



Published 52 publications to the Partner Portal.

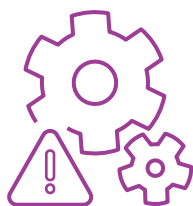


Published a total of 76 alerts, advisories and publications on cyber.gov.au, including a range of joint products with international partners.



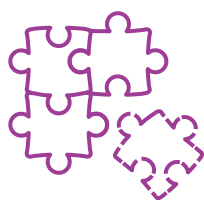
Cyber Hygiene Improvement Programs

- Distributed over 8,300 notifications identifying active cyber risks.
- Distributed over 14,000 reports to approximately 3,500 customer organisations.
- Distributed over 12,300 notifications of possible compromise to approximately 1,885 organisations.



Government Uplift Program

- There were 37 Cyber Uplift Remediation Program engagements.
- Completed 3 Government Cyber Assessment Team (GovCAT) assessments – identifying vulnerabilities and supporting critical functionality.
- Trained 9,955 participants in Privileged User Training.
- Uplifted 20 instances of commonly used cyber security software through their configuration.
- Assisted 8 entities with visibility and detection uplift.



Critical Infrastructure (CI) Uplift Program

- Completed 6 CI uplifts.
- Completed 12 CI uplift sprints.
- Held 10 technical cyber security workshops with CI operators.
- Reached 258 representatives from 157 CI organisations through Operational Technology Information Exchanges.

Year in Review

Timeline of key events and publications



July 2025	
09	<i>Protect Your Devices SMB Checklists</i> guidance published
30	<i>Scattered Spider</i> advisory published
August 2025	
14	<i>Foundations for OT Cyber Security</i> guidance published
26	<i>Managing Cryptographic Keys and Secrets</i> guidance published
28	<i>Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System</i> advisory published
September 2025	
4	<i>A Shared Vision of Software Bill of Materials for Cybersecurity</i> guidance published
12	<i>Information Security Manual</i> updated
22	<i>Planning for Post-quantum Cryptography</i> published
October 2025	
13	<i>CI Fortify</i> published
15	<i>Mitigations for Network Defence</i> published
16	<i>Machine Learning Supply Chain Risks and Mitigations</i> published
20	<i>Cloud Shared Responsibility Model</i> published
23	<i>Investing in Modern Defensible Architecture</i> published
28	<i>Creating and Maintaining a Definitive view of an Operational Technology Architecture</i> published
30	<i>Cyber Security Priorities for Boards of Directors 2025–26</i> guidance published
31	<i>Microsoft Exchange Security Best Practice</i> published
November 2025	
20	<i>Bulletproof Defence: Mitigating Risks from Bulletproof Hosting Providers</i> published

December 2025

- 4** *Principles for the Secure Integration of Artificial Intelligence in Operational Technology* published
- 4** *Information Security Manual* updated
- 10** *Pro-Russia Hacktivists Conduct Opportunistic Attacks Against US and Global Critical Infrastructure* advisory published
- 15** *Quantum Technology Primer for Cybersecurity Leaders* published

January 2026

- 14** *Artificial Intelligence for Small Businesses* published
- 15** *Secure Connectivity Principles for Operational Technology (OT)* published

February 2026

- 19** *Quantum Technology Primer: Computing* published

March 2026

- 5** *Artificial Intelligence and Machine Learning: Supply Chain Risks and Mitigations* published
- 6** *INC Ransom Affiliate Model Enabling Targeting of Critical Networks* published, marking the first time an ASD ACSC joint advisory was co-sealed with a Pacific Island Nation (the Kingdom of Tonga)
- 17** *Information Security Manual* updated
- 18** *Quantum Technology Primer: Communications* published
- 25** *Securing Space* published

April 2026

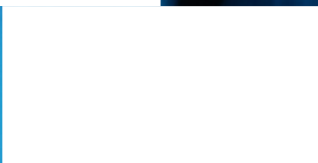
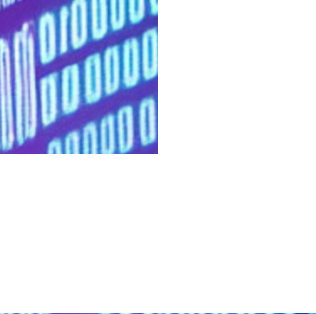
- 24** *Defending against China-nexus Covert Networks of Compromised Devices* published

May 2026

- 1** *Careful Adoption of Agentic AI Services* published
- 7** *ClickFix Distributing Vidar Stealer via WordPress Targeting Australian Infrastructure Advisory* published
- 27** *Opportunities for AI in Cyber Defence* published

June 2026

- 9** *Guidelines for System Hardening Advice* published
- 9** *Guidelines for Software Development Advice* published
- 9** *Information Security Manual* updated
- 22** *Five Eyes Cyber Security Agencies Statement* published
- 24** *Quantum Technology Primer: Sensing* published



Year in Review

ASD's ACSC categorises each cyber security incident it responds to on a scale of Category 1 (C1), the most severe, to Category 6 (C6), the least severe. Cyber security incidents are categorised on severity of impact and significance of the organisation's impact to Australia.

EFFECT	Denial of Essential Systems	0 C6	0 C5	0 C4	0 C3	0 C1	0 C1
	Extensive Incident	0 C6	9 C5	17 C4	13 C3	1 C2	0 C1
	Localised Incident	0 C6	15 C5	12 C5	12 C3	2 C3	0 C2
	Isolated Incident	2 C6	110 C6	58 C5	47 C4	22 C3	2 C3
	Low-level Malicious Incident	0 C6	174 C6	81 C5	117 C4	85 C4	2 C3
	Unsuccessful Low-level Malicious Incident	0 C6	28 C6	36 C6	194 C6	466 C6	19 C6
		Member(s) of the public	Small organisation(s); Sole traders	Medium-sized organisation(s); Schools; Local Government	State Government; Academia & R&D; Large organisation(s); Supply Chain	Federal Government; Government shared services; Regulated Critical Infrastructure	National Security; Systems of National Significance
SIGNIFICANCE							

FIGURE 1: Cyber security incidents by severity category for FY2025–26 (total 1,524).

Caveat: ASD's ACSC reviewed and updated the way it categorises cyber security incidents in FY2025–26 to improve accuracy; therefore, some incident categories will not align with last year.

FY2025–26 demonstrated that the cyber threat environment continues to be shaped by compromises from well known weaknesses such as unpatched systems and social engineering, while the operating environment continues to evolve. More interconnected systems, third party suppliers and supply chains mean one compromise makes incidents far more complex in this current environment. FY2025–26 also saw cyber security awareness growing and improved reporting practices across the economy.

In FY2025–26, ASD's ACSC responded to over 1,500 incidents, an increase of more than 20% from last year. Of the incidents ASD's ACSC responded to this year, 362 were identified following proactive ASD's ACSC notifications to entities of potential malicious activity on their network. In FY2025–26, ASD's ACSC issued over 4,400 notifications (including mass notifications) of suspicious cyber activity, almost 80% more than FY2024–25. More than 51% of individual notifications originated from declassified intelligence, providing reliable and actionable information directly to Australian organisations.

- A collective notification to 340 entities in May 2026 regarding the cPanel CVEs resulted in more than 60 confirmed incidents.
- ASD's ACSC received fewer phone calls reporting cyber security incidents this financial year; however, the number of incidents reported (including unsuccessful incidents) increased, which likely indicates improved cyber security awareness and reporting culture.

Incidents categorised as C3 or above often involve organisations such as federal and state governments, large organisations, academia and supply chains. While the number of higher categorised incidents decreased in FY2025–26 with only one C2 incident recorded, the number of extensive compromises increased from 26 in FY2024–25 to 40 in FY2025–26. Furthermore, analysis of MITRE ATT&CK tactics, techniques and procedures (TTPs) indicates an increasing complexity in depth and breadth of cyber tactics. Of note:

- The frequency of 'User Execution' and 'Social Engineering' techniques demonstrates that humans remain an enduring target for all incident categorisations.
- The high rate of 'Data Encryption for Impact' suggests that ransomware is a strong contributor to C3 and higher incidents in FY2025–26.

In previous years, major Denial of Service (DoS)/Distributed Denial of Service (DDoS) campaigns accounted for higher incident numbers; however, due to the absence of any coordinated DDoS campaigns by malicious cyber actors in FY2025–26, ASD's ACSC recorded lower numbers of DoS/DDoS incidents. ASD's ACSC responded to more than 80 incidents involving DoS/DDoS, down more than 60% from last year.

DoS/DDoS attacks remain a common tactic used to disrupt services and affect organisational operations. Although fewer incidents were reported, those that did occur resulted in more significant impacts. Extensive compromises from DDoS activity increased from one in FY2024–25 to seven in FY2025–26.

ASD's ACSC is consistently seeing cyber security incidents resulting from unpatched vulnerabilities. This year, ASD's ACSC recorded successful exploitation of a vulnerability identified in 2008, demonstrating the need to patch legacy vulnerabilities, as well as keeping on top of patching new ones. AI is reducing the expertise and effort required to identify and exploit vulnerabilities, likely accelerating Time to Exploit (TTE) and increasing the number and diversity of actors able to undertake cyber attacks.

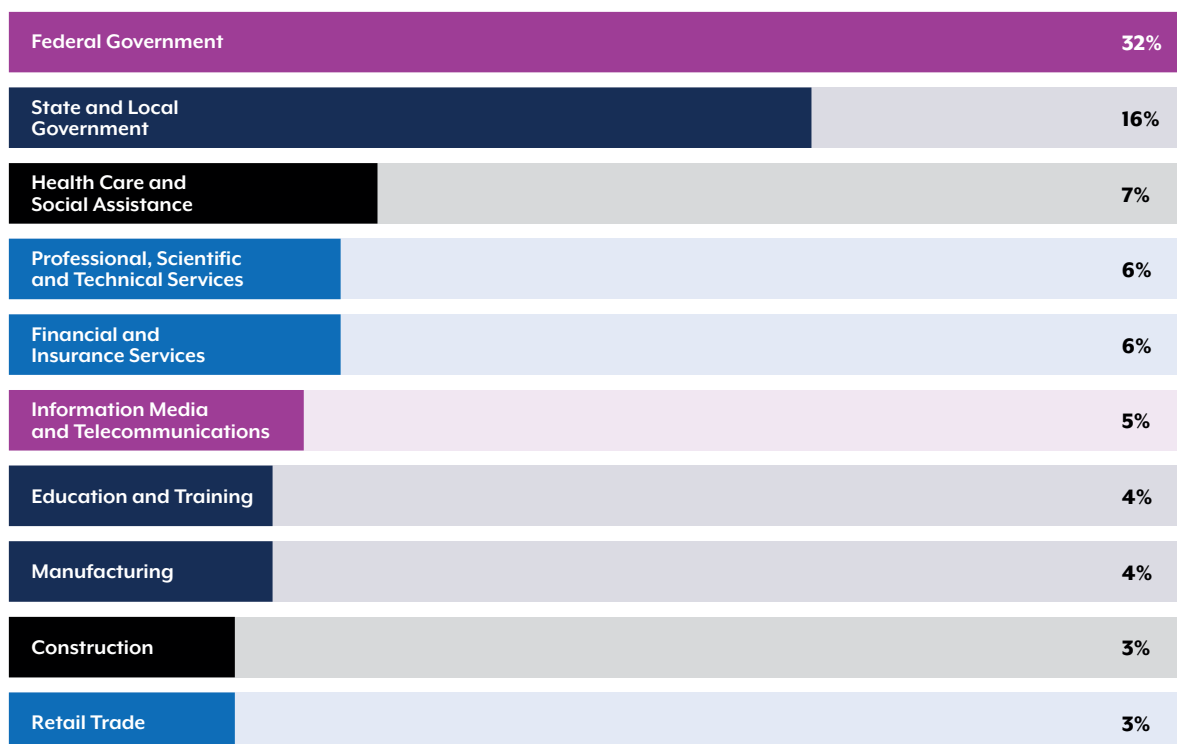
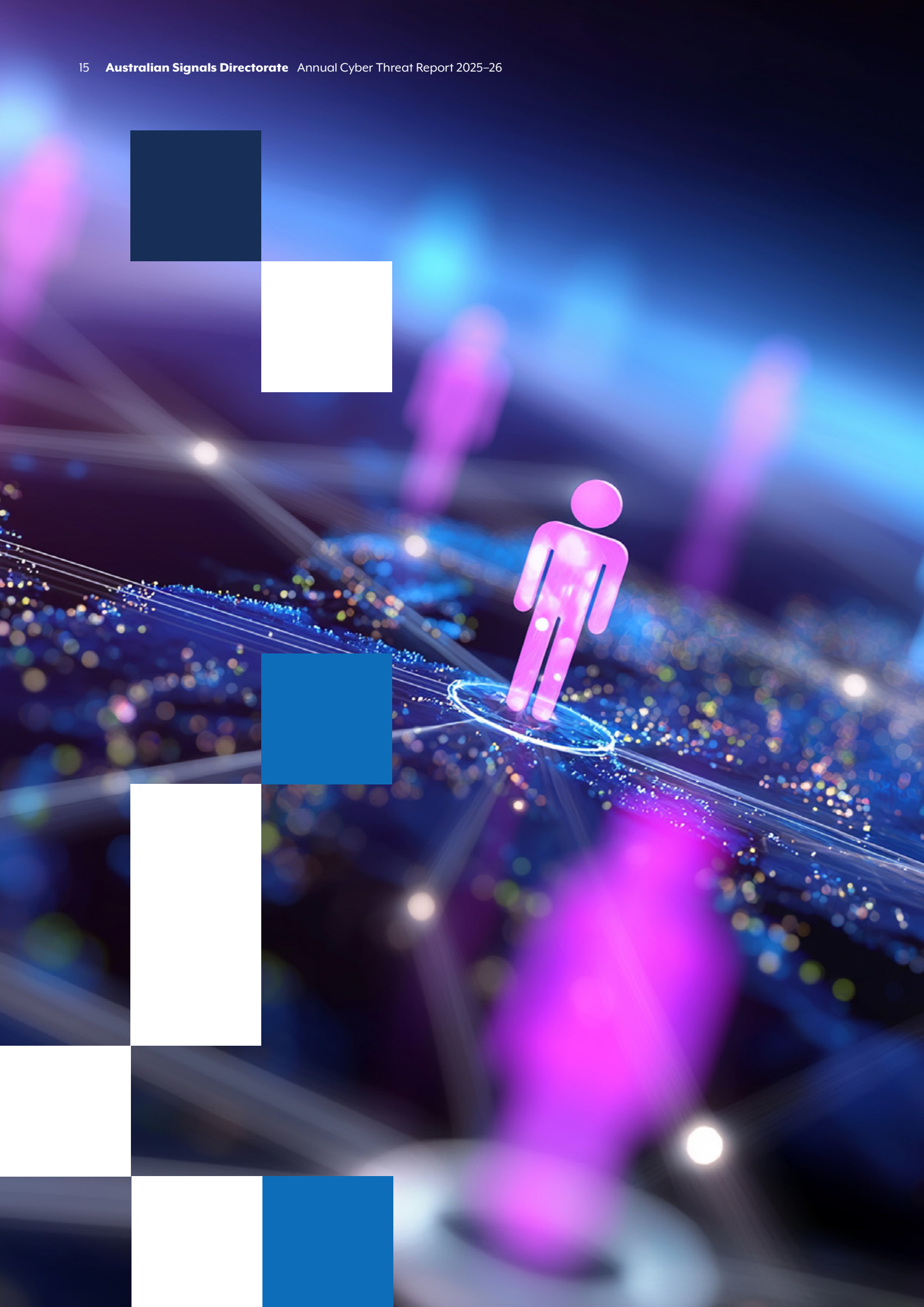


FIGURE 2: Top 10 reporting sectors from incidents reported to ASD's ACSC

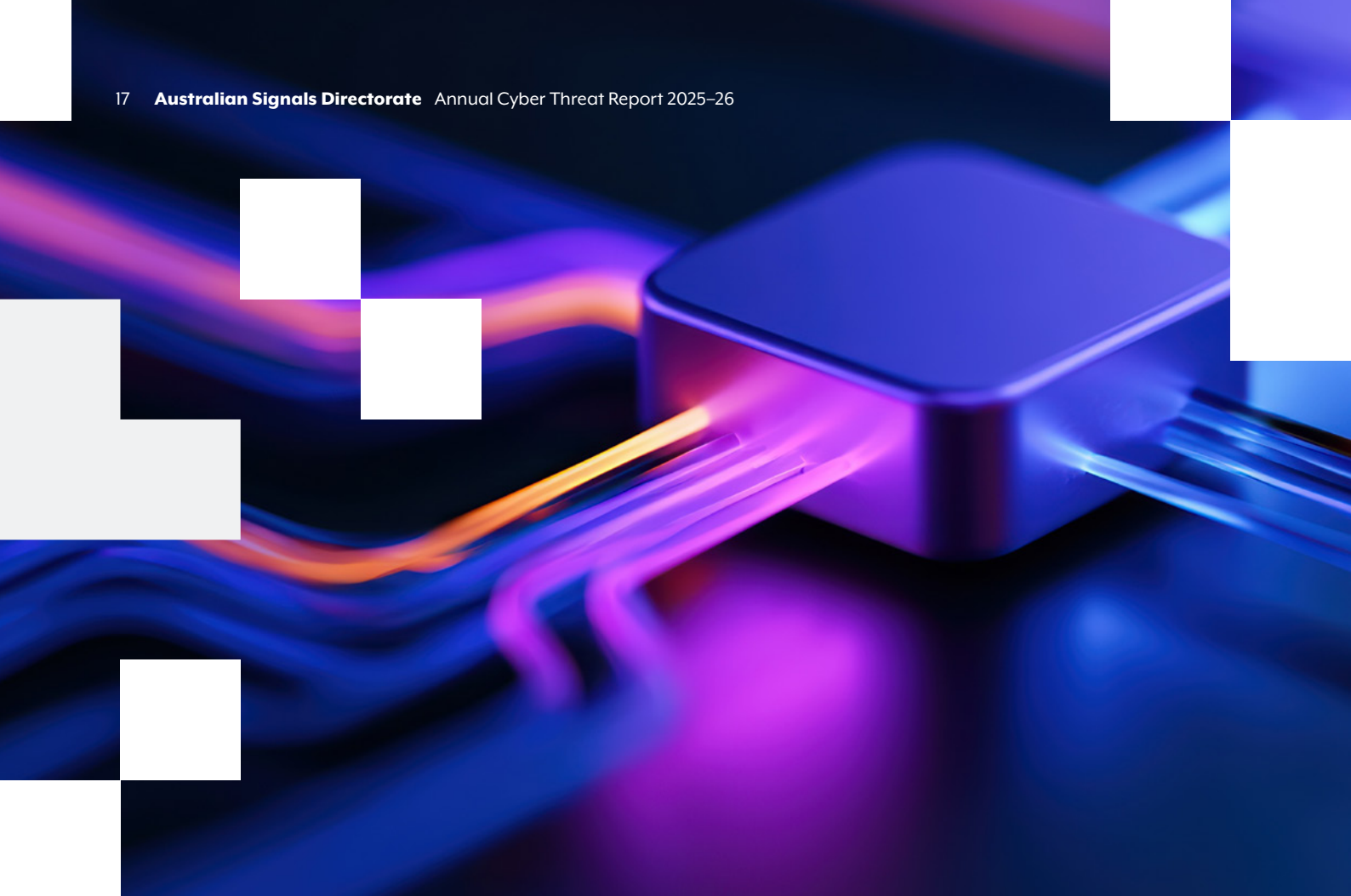
Note: ASD's ACSC categorises sectors following the Australian and New Zealand Standard Industrial Classification (ANZSIC) Divisions from the Australian Bureau of Statistics.

In FY2025–26, Government again reported the highest number of incidents, led by the Federal Government, likely due to Government's additional reporting obligations. Of note, Health Care and Social Assistance rose to be the most frequently reporting non-government sector, followed by Professional, Scientific and Technical Services. This year saw the emergence of the Manufacturing sector into the top 10, having the largest increase in incident reports across all sectors, while Transport dropped out of the top 10.



Australian cyber threat landscape

- Australia's prosperous economy and advanced digital infrastructure make it an attractive target for malicious cyber actors seeking to advance their financial, political and strategic interests.
- Recent global conflicts have demonstrated that cyber capabilities are now regularly integrated by state-sponsored actors, and those aligned with their cause, to support military objectives, disrupt critical systems and shape the strategic environment.
- State actors continue to target Australian governments, businesses, and CI to conduct espionage and gain strategic advantage. Some are motivated to maintain access covertly to disrupt essential services during periods of crisis or conflict.
- Cybercrime remains a significant threat to Australia's prosperity and way of life. Cybercriminals are prepared to sell our data online or disrupt services to elicit payment.



Malicious use of AI

AI will help us improve cyber defence over time; however, it also accelerates the speed, scale and sophistication of cyber threats. These technologies can generate text, code, images and video, and automate repetitive or complex tasks to improve efficiency and productivity. However, as Australian organisations integrate AI and large language models into their environments, new and potentially exploitable security risks are emerging, expanding their overall opportunities – or our attack surface.

Over the last financial year, ASD's ACSC has observed the increased risks and exposure that advances in AI models have introduced into Australian organisations.

Social engineering

Social engineering is a longstanding and evolving threat to individuals and organisations within Australia, and one that enables malicious cyber actors to compromise accounts, devices, systems or sensitive information.

Malicious cyber actors often go to great lengths to make their communication seem legitimate and trustworthy, increasing the chances that a targeted person will follow their instructions. Recent advancements in AI have amplified the effectiveness of social engineering techniques. For example, malicious cyber actors can use AI to write effective phishing emails, free from grammar and spelling errors, and automate targeted spearphishing attacks. To achieve their goals, malicious cyber actors have weaponised empathy, urgency, and trust to trick individuals or staff into circumventing regular processes to achieve their goals. These communications may appear to come from someone known to the victim, such as a relative, colleague, or senior manager, or an authoritative part of their organisation. AI lowers the skill barrier and increases scale, but does not fundamentally change the nature of social engineering attacks.

While social engineering attempts can be received by anyone, malicious cyber actors often prioritise individuals who have access to sensitive information, the ability to make changes to systems, the authority to perform financial transactions, or those whose roles require regular interaction with unknown or external parties. Anyone can be a target of social engineering, from an employee to the CEO.

The Australian Securities and Investments Commission (ASIC) has seen a sharp rise in online scams using deepfake videos of celebrities and politicians to encourage Australians to part with their money, with criminals increasingly exploiting topical issues in the news to deceive consumers. In June 2026, an Australian broadcaster publicly reported that scammers generated a fake version of their website, along with misleading articles and false images of prominent Australians, to advertise a fraudulent investment platform.

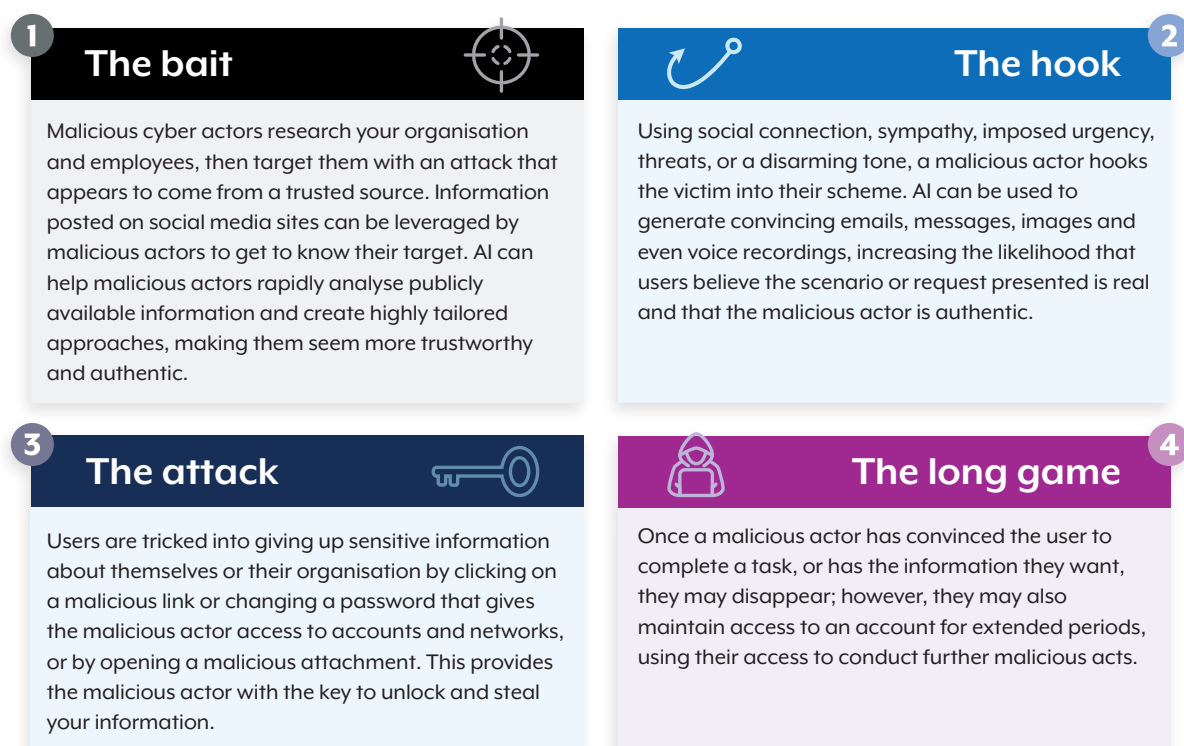


FIGURE 3: How social engineering attacks are commonly conducted

Vulnerability discovery

As technology becomes increasingly embedded in Australian lives and businesses, the number of potential vulnerabilities for malicious cyber actors continues to grow. Malicious cyber actors often exploit security weaknesses in IT systems, known as common vulnerabilities and exposures (CVEs), to gain unauthorised access, steal data, or take control of a system. The assistance of AI tools can accelerate the ability to exploit vulnerability chains, where multiple weaknesses are linked together to gain broader access.

Vulnerabilities can include software bugs, system misconfigurations or insecure processes that malicious cyber actors might be able to take advantage of to harm an organisation. Although many vulnerabilities exist, only some pose significant risks.

AI may enable the faster identification and analysis of vulnerabilities in systems and software, reducing the time, effort and skill required of malicious actors. AI systems can be used to automate data collection and analysis, which allows for automated reconnaissance, data collection, and effective target selection. Likewise, over-optimisation, ambiguous instructions, poorly enforced boundaries and the ability to exploit software vulnerabilities or security control weaknesses can increase the risk that AI tools take unsafe or unexpected actions.

ASD's ACSC has previously observed that most vulnerability exploitation occurs within two weeks, with some CVEs successfully exploited within 48 hours of a patch or mitigation advice being released. Over the next 12 months, the growth of AI-driven tools will further compress this window. This accelerated timeline highlights the increasing speed and efficiency of malicious actors' operations, leaving organisations with less time to detect, patch and respond to newly disclosed vulnerabilities. The gap between vulnerability disclosure and its exploitation has never been narrower. In the past, defenders had months to patch, now they have days, sometimes only hours. Combined with automated tools and pre-existing exploit kits to quickly code, test and deploy, proof of concepts can significantly shorten the window between disclosure and active exploitation.

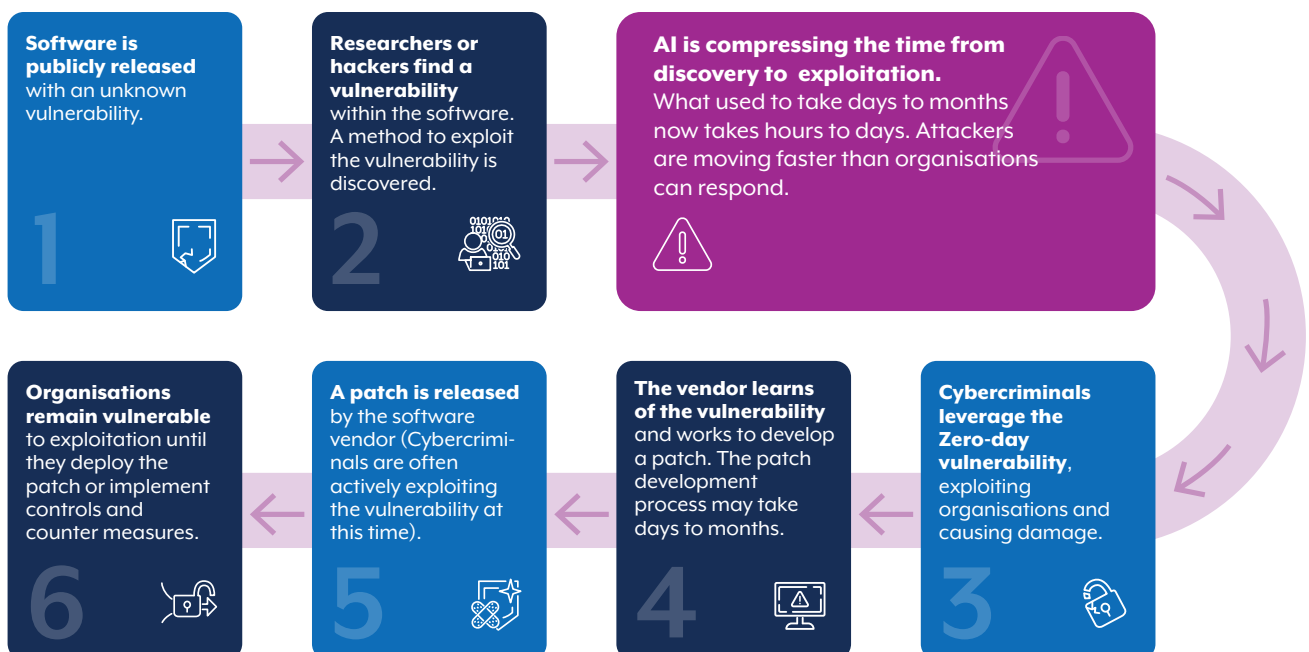


FIGURE 4: Time to Exploit



Data mining and extraction

ASD's ACSC has observed cybercriminals rapidly acquiring public and stolen data to extract useful information – such as usernames and passwords – to accelerate their activities. Some AI tools can scrape social media and public sources to quickly profile victims for future malicious cyber activity – such as identity theft, fraud and social engineering attempts.

According to public reporting, in 2025, a US-based AI company disrupted a cybercriminal group that used their AI to generate code for the theft and extortion of personal data at scale. The actor used the AI to semi-automate aspects of their operation from reconnaissance to network compromise. The AI also obtained and analysed financial data from victim organisations to determine a ransom amount. Although the effectiveness of the attack is not clear, this example demonstrates how AI may be used by malicious cyber actors.

State-sponsored actors

Great power competition and escalating geopolitical tensions are reflected in cyberspace. Over the 2025–26 financial year, Australia continued to experience persistent reconnaissance and testing of government and privately owned networks by state-backed actors.

State-sponsored actors have targeted Australian organisations, primarily to gain access to sensitive, or non-public information — not limited to government information. State-sponsored actors actively pursue information that can assist to fill their own intelligence gaps and to reduce their tactical, operational, strategic and commercial risk. This information can include data associated with individuals, operations, or organisational governance. This information is not exclusively held by governments and can almost certainly be gleaned from the networks of CI entities, private businesses, and individuals.

In the Indo-Pacific, state-sponsored actors are possibly preparing for eventualities, such as crisis or conflict, by pre-positioning capabilities for disruptive effects, or to access higher-value target networks to use at the time of their choosing. State-sponsored actors can use disruption to achieve strategic goals, such as limiting the ability to respond to an event or cause social unrest.

State-sponsored actors use a range of techniques to target Australian entities. State-sponsored actors will use low-effort or low-cost techniques to conduct opportunistic attacks and reserve advanced capabilities for high value targets.



CASE STUDY 1: DEFENDING AGAINST CHINA-NEXUS COVERT NETWORKS OF COMPROMISED DEVICES

In April 2026, ASD's ACSC joined international partners in highlighting the major shift in the TTPs used by China-nexus cyber actors.

There has been a recent widespread change in the TTPs used by China-nexus cyber actors, moving away from the use of individually procured infrastructure, and towards the use of externally provisioned, large-scale networks of compromised devices.

Most China-nexus threat actors are believed to be using these covert networks. Multiple covert networks have been created and are regularly updated, and a single covert network could be used by multiple actors at one time. These networks are primarily made up of compromised Small Office Home Office routers, as well as Internet of Things (IoT) and smart devices.

Covert networks are used to connect across the internet in a low-cost, low-risk, deniable way, disguising the origin and attribution of malicious activity. These networks are used against targets of espionage and offensive cyber operations for each phase of the Cyber Kill Chain; from reconnaissance and malware delivery to command and control and data exfiltration.

Defending from attackers using covert networks will be different based on resourcing and the nature of the target organisation. All organisations should map and baseline their edge device traffic, especially VPN remote access connections, and adopt dynamic threat feed filtering that includes known covert network indicators. The advisory contains further specific guidance for small, medium and large organisations.

For more information, see *Defending against China-nexus covert networks of compromised devices* on cyber.gov.au.



Cybercriminals

Cybercrime continues to be a pervasive threat to Australia's economic and social prosperity. Cybercrime is persistent and damaging across all facets of Australia's economy as cybercriminals are willing to exploit opportunities for profit. The online domain has become an integral and ubiquitous part of daily life; with digital infrastructure and the information that companies hold being prime targets for cybercriminals.

Cybercriminals target Australian individuals and organisations for financial gain, attempting to conduct extortion, often using ransomware attacks or data theft. In the 2025–26 financial year, ASD's ACSC received over 82,000 cybercrime reports through ReportCyber; however, it is likely that most cybercrime goes unreported.

Data theft

Data theft remains an ongoing and serious threat to Australians. PII – such as date of birth, email address and Medicare number – is highly valuable to cybercriminals, who exploit it as a commodity. Cybercriminals also use PII as a target to be acquired for other purposes, including the planning and execution of further criminal activities. For example, stolen PII can be used or sold on the dark web, aiding identity theft schemes and additional cyberattacks.

The average self-reported cost of cybercrime overall was \$38,130 – with identity fraud, online shopping fraud, and online banking fraud the most frequently reported cybercrime types.

Of the cyber security incidents recorded by ASD's ACSC during FY2025–26, 98 were data breaches, accounting for over 6% of all incidents. This was an increase of 66% in data breach incidents compared to the previous year.

CASE STUDY 2: MULTI-STAGE SOCIAL ENGINEERING – SCATTERED SPIDER

On 30 July 2025, ASD's ACSC and international partners released an updated joint advisory in response to recent activity by Scattered Spider threat actors against commercial facilities sectors, subsectors and other sectors.

Scattered Spider threat actors typically engage in data theft for extortion and use several ransomware variants, most recently deploying ransomware alongside their usual TTPs. While some TTPs remain consistent, Scattered Spider threat actors often change TTPs to remain undetected.

Scattered Spider has been observed researching organisations to identify usernames, passwords, PII, and to conduct SIM swaps. The threat actors then use layered social engineering techniques which frequently occur over several calls. The social engineering attempts are designed to first learn what steps are needed to conduct password resets from helpdesks. Once that information is identified, the threat actors continue to conduct phone calls to employees and help desks to gather password reset specific information of a targeted employee.

Finally, the threat actors conduct spearphishing calls to convince IT help desk personnel to reset passwords and/or transfer multi-factor authentication tokens. At which point, the threat actors perform account takeovers against the users in single sign-on environments. These social engineering attempts are enriched by access to personal information derived from social media, open-source information, commercial intelligence tools, and database leaks.

HIGHLIGHT 1: OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER (OAIC) NOTIFIABLE DATA BREACH SCHEME

2025 marked the highest number of notifications in a year since the OAIC's *Notifiable Data Breaches* scheme commenced in 2018, with 1205 breaches.

Between July and December 2025, malicious or criminal attacks accounted for 405 of the overall number of breaches, remaining the largest source of data breaches for that reporting period.

This was particularly significant within the health sector, which reported 64 notifications of this nature during the 6-month period. Cyber security incidents can have significant impacts on individuals, and organisations need to remain vigilant and alert to the risks.

The OAIC does not take regulatory action in response to every data breach. Instead, they direct efforts to where they can have the greatest impact and to where there is the largest risk of harm to the community. There is more detail in their *Statement of regulatory approach* at [oaic.gov.au](https://www.oaic.gov.au).

Ransomware

Ransomware continues to stand out as one of the most disruptive, costly and persistent cyber challenges facing Australia in FY2025–26. Over the past decade, ransomware has evolved from using basic encryption and extortion into an interconnected ecosystem where cybercriminals communicate and conduct payments through borderless online spaces that makes investigating cybercrime difficult. Cybercriminals often use ransomware to encrypt information, including PII, and demand a ransom to prevent the information from being leaked or sold online.

In FY2025–26, ASD's ACSC responded to 139 ransomware incidents, a figure consistent with the previous year. While the 3 ANZSIC divisions most affected by ransomware, Health Care, Professional, Scientific and Technical Services, and Manufacturing, remained unchanged, the severity of incidents increased, with extensive ransomware incidents rising from 16 to 24.

The growth of the Cybercrime-as-a-service (CaaS) 'business model' has made cybercrime more accessible, scalable and efficient. This means that less skilled cybercriminals can access ready-made malware and infrastructure, increasing the number of malicious cyber actors in cybercrime. AI is also streamlining processes across the CaaS ecosystem, making cybercrime faster, less expensive and more effective than ever before.

Ransomware developers are responsible for the creation, upkeep and improvement of ransomware products. Commonly seen in the Ransomware-as-a-Service (RaaS) model, ransomware affiliates can purchase and customise ransomware for their attacks, then share a percentage of the profits with the RaaS developer. Payments to developers can also include rental or subscription-based services.

Paying a ransom does not guarantee recovery of ransomed data, nor prevent it from being sold or leaked online. Paying a ransom also helps promote ransomware as a profitable criminal enterprise. For more information, visit <https://www.cyber.gov.au/threats/types-threats/ransomware>

HIGHLIGHT 2: INC RANSOM

In March 2026, ASD's ACSC in collaboration with international partners – Kingdom of Tonga's National Computer Emergency Response Team (CERT Tonga) and New Zealand's National Cyber Security Centre (NCSC) – released a joint advisory on the ransomware group, INC Ransom.

INC Ransom is a financially motivated cybercriminal group that provides a RaaS operation to its affiliate network. The group and its affiliate network have previously targeted the US and UK; however, since early 2025, they have been increasingly observed targeting Australia, New Zealand and the Pacific Island states.

In mid-June 2025, the Tongan Ministry of Health (MoH) was impacted by a ransomware attack that rendered core services inaccessible and disrupted the national health care network. INC Ransom later claimed responsibility for the attack.

INC Ransom affiliates use double extortion tactics. Affiliates steal sensitive data, encrypt files, and threaten to publish stolen data, via their data-leak site, to pressure organisations into paying the ransom. The affiliates rely on compromised credentials or public-facing vulnerabilities for initial access into the victim's networks. For more information, see *INC Ransom Affiliate Model Enabling Targeting of Critical Networks*.

HIGHLIGHT 3: MEDIA LAND SANCTIONS

In November 2025, the Australian Government imposed targeted financial sanctions, under the Autonomous Sanctions Regulations 2011, against 2 Russian cybercrime service providers – Media Land LLC and ML. Cloud LLC – and 2 of their key personnel – Aleksandr Alexandrovich Volosovik and Kirill Andreevich Zatolokin. These sanctions were in response to these organisations' provision of ransomware infrastructure to malicious cyber actors and cybercriminals, allowing them to conduct cyber attacks in Australia and around the world. In Australia, these attacks were conducted against Australian financial institutions, Australian businesses and their customers, and international CI.

Australia's cyber sanctions are strengthened by trilateral sanctions imposed by the US and UK against these malicious cyber actors, demonstrating our collective resolve to combat cybercrime.

This is the fifth time we have activated Australia's autonomous cyber sanctions framework, part of the Australian Government's coordinated action against cybercrime. These latest sanctions make it a criminal offence to provide assets to either Media Land entity or the 2 sanctioned individuals, or to use or deal with their assets, with penalties of up to 10 years' imprisonment and/or heavy fines. These sanctions also ban the individuals from entering Australia.

Malicious cyber actors will persistently target Australian governments, CI, businesses and individuals. This threat will continue to be met by the collaborative work of the AFP, ASD's ACSC, DFAT, and the whole of government through Australia's autonomous cyber sanctions framework. Cyber sanctions are a key tool to disrupt and deter malicious cyber actors and protect Australians from this threat.

Cyber in modern conflict

Australia continues to face a complex set of strategic circumstances. New conflicts in the Middle East and ongoing conflict in Ukraine are fueling international instability – contributing to economic uncertainty and supply chain shock.

A range of actors, including state-sponsored actors, can use cyber means to achieve geostrategic, political or military effects during crisis or conflict. Malicious actors can conduct cyber operations at scale, which allows them to lay low in networks and generate effects across borders. These characteristics are increasingly valuable during a period of global instability.

The distinction between state-sponsored and cybercriminal activity continues to blur. Despite differing objectives, both often exploit the same vulnerabilities and use similar TTPs to compromise systems and extract data. This includes the use of AI.

EXPLAINER 1: AUSTRALIA'S STRATEGIC ENVIRONMENT

As the *2026 National Defence Strategy* identifies, threat deteriorating trends in Australia's strategic environment have broadened and intensified. The international system is under greater strain than at any time since the end of the Cold War. New strategic challenges have emerged that further threaten Australia's security and complicate the pursuit of Australia's interests. The global rules-based order, which has underpinned Australia's security and prosperity for decades, is in transition.

Intense competition between major powers – principally the US and China – will be an enduring feature of our strategic environment. Authoritarian regimes are also becoming more willing and able to disrupt CI, conduct cyber intrusions and engage in misinformation and disinformation campaigns. Malicious state and non-state-sponsored actors are continuing to improve their cyber capabilities, increasing the risk of disruptions to Australia's critical systems, infrastructure and networks.

State-sponsored actors in modern conflict

State-sponsored actors have demonstrated both their capability and intent to use cyber as a disruptive and destructive tool in crisis or conflict. Modern conflicts have highlighted how militaries incorporate cyber effects to enable or facilitate operations. They also use cyber as a tool to shape or influence conditions in their area of operations to better suit their desired outcome.

State-sponsored actors are investing in disruptive cyber capabilities for future use in conflict. They can commit the necessary time and resources to gain access to a victim's network and pre-position for future operations.

Hacktivists in modern conflict

Hacktivists are increasingly likely to pose a disruptive cyber threat to government and private sectors during crisis or conflict. While hackers are non-state-sponsored actors, they can also be patriotically motivated – targeting those whom they perceive as a threat to their own nation's geopolitical objectives. The increasingly unpredictable and volatile international environment is motivating hackers to target entities or states whom they deem are adversarial to their ambitions.

Hacktivists are becoming increasingly willing to engage in disruption activities that pose a threat to Australia, regardless of whether hackers deliberately target the Australian entity itself. Australia's geographical position in the Indo-Pacific places us at the forefront of many emerging global issues. Like other actors, hackers will likely benefit from emerging technologies, such as AI, to grow their capabilities and pose a bigger disruption threat to Australian sectors. Additionally, as Australia is heavily reliant on international supply chains, hacker disruption can affect Australia even if we are not the direct target.

- On 11 March 2026, Iranian hackers claimed responsibility for compromising Stryker, a US-based company that regularly imports surgical and pharmaceutical equipment into the Australian market. The group claimed this attack was in response to a US military strike in Iran. Although Australia was not directly targeted or impacted by this activity, the example highlights how Australia's complex supply chain nevertheless exposes it to hacker activity, even if that activity does not directly target Australia.
- On 10 December 2025, ASD's ACSC, alongside international partners, released an advisory assessing that pro-Russia hacker groups were targeting CI. They exploited insecure internet-facing virtual network computing (VNC) connections to infiltrate, or gain access to, operational technology (OT) systems. While these groups are generally less sophisticated and impactful than Advanced Persistent Threat (APT) actors, their activities have resulted in operational disruptions – including physical damage. Targeted sectors include water and wastewater systems, food and agriculture, and energy.

What malicious actors are targeting

Everyone can be a target

Cyber threats affect Australians of all ages, industries and communities. Criminals are increasingly combining cyber techniques with social engineering to scam, defraud and exploit individuals at scale.

Who is being impacted?

Highest reporting age groups



- 25-34 and 35-44 year olds accounted for **42%** of all scam reports to ReportCyber.

Youth reporting increased



- Reports from victims aged 17 and under increased **15%**.
- 48%** of reports related to cyber abuse.

Older Australians



- Reporting from Australians aged 65 and over decreased by **17%**.
- 51%** of reports accounted for online fraud activity.

Cybercrime in Australia 2025 report

Australian Cybercrime Survey 2025

- 64%** experienced cybercrime at some point in their life.
- 45%** were victims in the previous 12 months.

Most common cybercrimes

- 21%** malware
- 21%** identity crime and misuse
- 11%** fraud and scams



Why Australians remain vulnerable

Research conducted as part of the Australian Government's

Act Now. Stay Secure. campaign found:

- 57%** do not review privacy or location settings.
- 64%** have personally identifiable information visible on social media.

Password habits create risk

- 55%** reuse passwords across multiple accounts
- 59%** use variations of the same password
- 30%** include personal information in passwords

These behaviours make credential theft and account compromise easier for cybercriminals.



Four simple ways to be a harder target

- 1 Review privacy settings
- 2 Enable multi-factor authentication (MFA)
- 3 Use unique passwords or passkeys for every account
- 4 Think carefully before sharing personal information online



Cybercriminals increasingly exploit personal information and human trust. Simple cyber security practices can significantly reduce an individual's risk of becoming a victim.

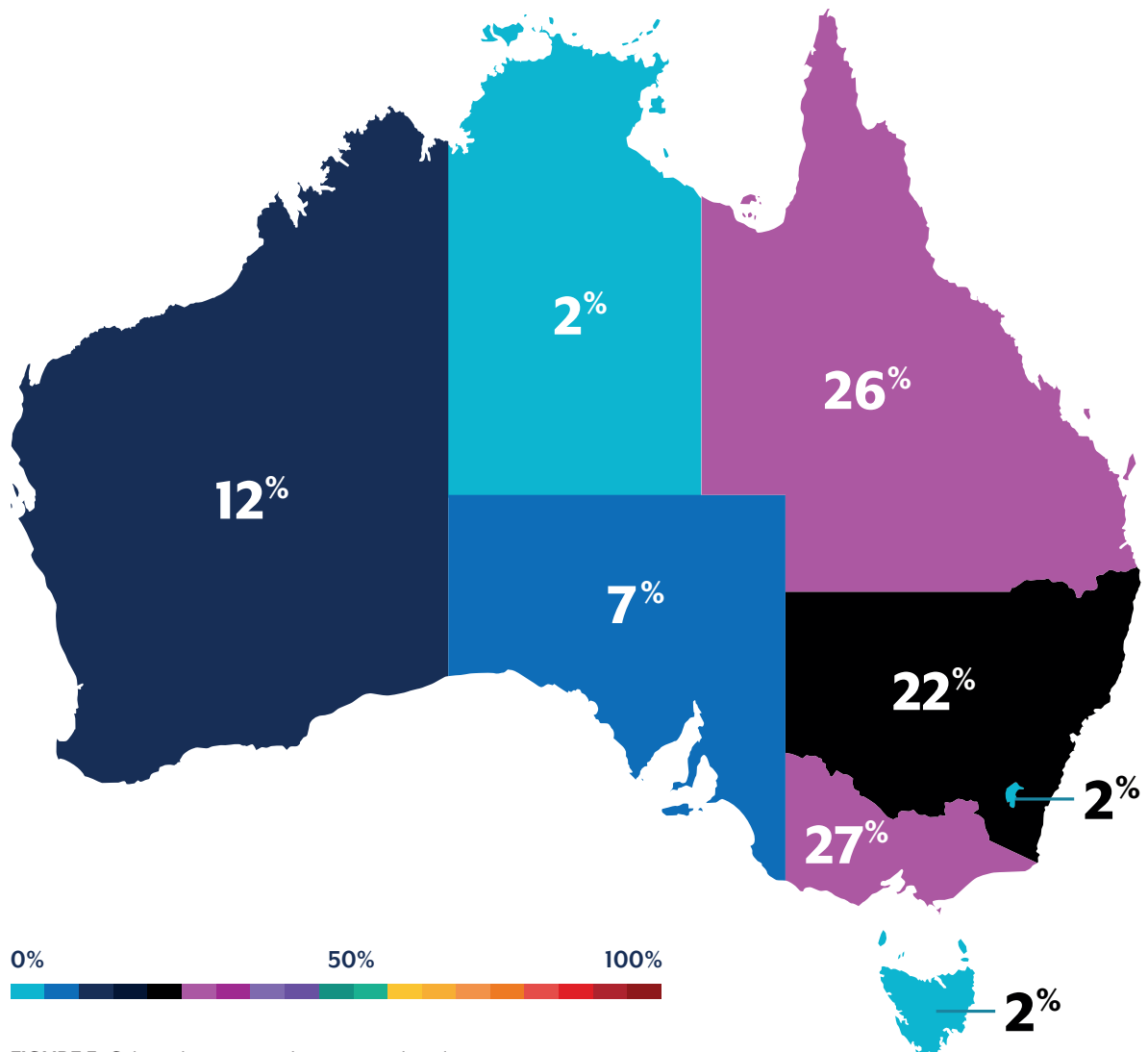


FIGURE 5: Cybercrime reports by state and territory

Australia's more populous states – Victoria, Queensland and New South Wales – continue to report more cybercrime than any other state or territory, with disproportionately higher reporting rates relative to their populations.



Critical infrastructure

CI continues to be an attractive target for malicious cyber activity due to the valuable data it holds and the important role it plays in everyday life. Malicious cyber actors seek to exploit CI for various reasons, ranging from financial extortion to espionage. A cyber attack affecting CI could undermine key sectors' functionality, including health and energy – causing operational disruptions and service shutdowns affecting millions of Australians.

In FY2025–26, CI incidents accounted for 10% of all incidents, similar to last year. ASD's ACSC responded to 154 CI incidents, a decrease of almost 7% compared to the previous year.

The top 3 MITRE ATT&CK initial access techniques leading to CI-related incidents were:

- Phishing (36%) – Adversaries used malicious emails, messages or other communications to deceive users and gain initial access to systems or credentials.
- Valid Accounts (16%) – Adversaries obtained and misused legitimate user accounts to access networks and systems without triggering traditional security controls.
- Drive-by Compromise (10%) – Adversaries gained access when a user visited a compromised or malicious website, resulting in the unintended download or execution of malicious content.

Top 3 ANZSIC divisions for CI incidents:

- Financial and Insurance Services (30%)
- Public Administration and Safety (21%)
- Electricity, Gas, Water and Waste Services (17%)

Cybercriminals continue to opportunistically target CI operators. CI is an attractive target for cybercriminals seeking to extort victims due to the sensitivity of the data stored by these entities, and the criticality of their services.

State-sponsored cyber actors routinely target Australia's CI networks, possibly to conduct espionage to gain a competitive and strategic advantage, or to pre-position for disruptive and destructive cyber effects against OT in the event of crisis or conflict. In crisis or conflict, access to an OT network could provide a malicious cyber actor with control over that infrastructure.

The following state-sponsored actors linked to the People's Republic of China (PRC), Russia, and the Democratic People's Republic of Korea (DPRK) have targeted Australia or its allies.

CI Fortify is ASD's ACSC guidance for Australian CI operators to strengthen cyber resilience and prepare for cyber incidents, disruptions, and other threats to essential services. Building resilience is essential to protecting critical systems and maintaining the delivery of services that Australians rely on every day. For more information, visit cyber.gov.au.

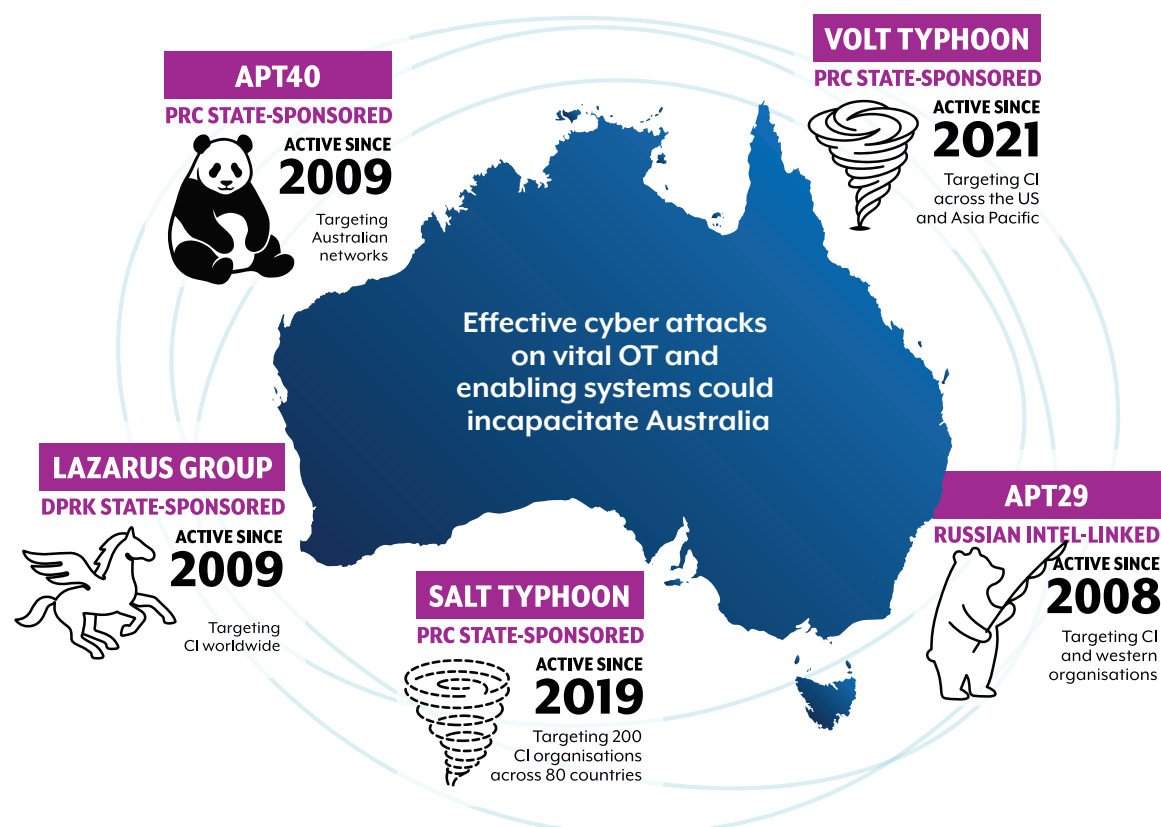


FIGURE 6: Effective cyber attacks on vital OT and enabling systems could incapacitate Australia. For more information, see CI Fortify.

HIGHLIGHT 4: COORDINATING THE FINANCIAL SECTOR AND NATIONAL CYBER RESPONSE

The cyber-attack response protocol (CART) helps coordinate the response to significant cyber incidents affecting Australia's financial system by bringing together APRA, ASIC, the Reserve Bank of Australia and Treasury to share information, maintain situational awareness and support a common operating picture. The mechanism helps ensure that actions to maintain financial stability and the continuity of critical financial services are aligned across financial sector authorities.

During significant cyber incidents, CART supports coordination between financial sector response arrangements and broader Australian government cyber incident management frameworks. This helps align financial sector actions with national cyber response activities led by relevant agencies, including ASD's ACSC and the Department of Home Affairs, ensuring regulatory, supervisory and operational responses are coordinated during incidents with potential cross-sector or national consequences.

By connecting financial sector authorities with broader government response arrangements, CART strengthens preparedness, supports timely decision-making and helps Australia respond more effectively to cyber incidents that could threaten critical financial services, financial stability or broader national interests.

CASE STUDY 3: AUSTRALIAN BANK REPORTS VISHING ACTIVITY

In August 2025, a bank reported to ASD an incident involving two phone calls to its internal help desk, in which the callers impersonated staff members to obtain information.

The callers impersonated a Melbourne-based employee, using staff details such as the employee's ID number, and claimed they were unable to connect with colleagues via Microsoft Teams. The calls indicated that the threat actor had conducted prior intelligence gathering on the organisation. Questions focused on a specialised financial services team located in Melbourne and Sydney and demonstrated insider knowledge.

The threat actors were manipulative, confrontational, and aggressive throughout the phone calls, employing a range of social engineering techniques to pressure help desk staff into compliance. They successfully obtained names, job titles, and corporate phone numbers for several staff members, potentially exposing employees to increased targeting by social media, and exposing the bank to an increased likelihood of follow-on attacks. The bank noted that the targeted team and individuals were not public figures and this lack of visibility made it easier for the threat actors to manipulate help desk staff, as the staff did not immediately perceive the requests as suspicious.

During its investigation, the bank determined that the calls likely originated from a call centre or office environment, as multiple voices were audible in the background. Furthermore, the calls were not made using Voice over IP (VoIP) technology and were confirmed to have originated from Hong Kong. Recent media coverage of vishing tactics targeting help desks prompted the bank to report the incident to ASD.

Since the incident, the bank's cyber security team has led an awareness campaign and supported team leads with additional training. Incidents involving elements of social engineering remain common in reports to ASD as threat actors leverage vulnerabilities wherever they exist, technical or human.

Report a cybercrime or cyber security incident at cyber.gov.au/report

or call the 24/7 Australian Cyber Security Hotline on **1300 CYBER1 (1300 292 371)**

HIGHLIGHT 5: CYBER ARROW

In October 2025, ASD's ACSC National Exercise Program delivered a national multi-sector operational cyber security exercise, Exercise Cyber Arrow (ECA). ECA involved multiple sectors from across Australia's CI, including over 175 energy, communication, financial services and market sector organisations, and government entities.

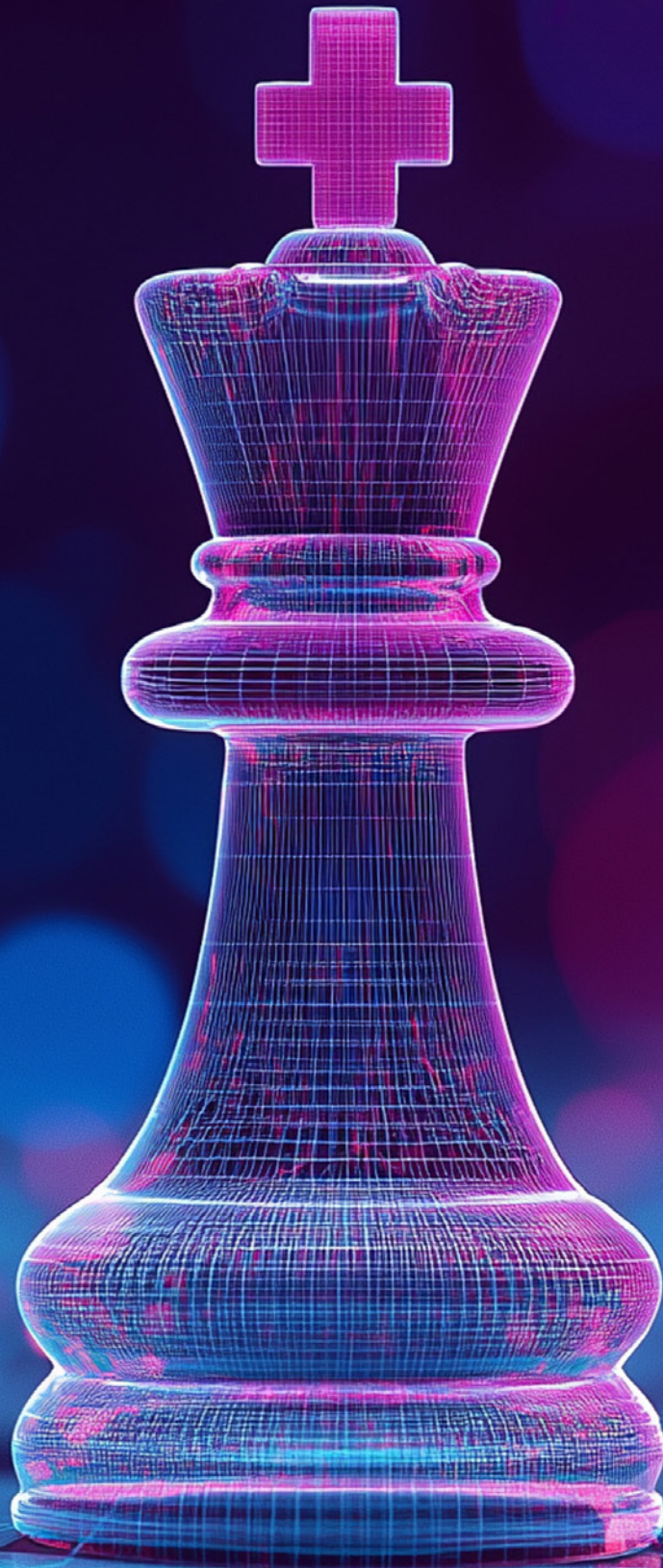
The exercise provided technical and operational teams with the opportunity to get hands-on experience detecting and responding to a cyber incident, and enabled participants to validate and improve their cyber incident response plans and playbooks. Participants highlighted that the functional exercise environment enabled robust testing of protocols under conditions reflective of real-world operational complexity. The integration of adversary-modelled TTPs into the scenario strengthened participants' capability to identify, mitigate, and proactively hunt for APT adversaries in real time, providing valuable insights into advanced detection and response practices.

ECA demonstrated how vital it is for CI sectors and government to work seamlessly together sharing intelligence, maintaining situational awareness, and responding decisively under pressure — to contain and manage a complex multi-sector cyber incident.

'Cyber threats to Australian infrastructure require a coordinated national response, reinforcing the importance of initiatives like Exercise Cyber Arrow in driving continuous improvement in incident response. Through a practical, hands-on environment, Horizon Power was able to validate its detection and response capabilities and confirm the maturity of its incident response processes, while also identifying areas requiring further enhancement. Collaborative national exercises of this nature play a critical role in strengthening organisational readiness and contributing to a more resilient and prepared Australian cyber security ecosystem.' Horizon Power.

'ASD's Cyber Arrow Exercise reinforced the importance of continued collaboration between government and industry to help strengthen Australia's cyber resilience. It demonstrated the coordination and continued focus required to respond effectively to significant cyber events. ANZ supports initiatives that bring together cross-sector partners to enhance collective preparedness.' ANZ

ASD encourages organisations to conduct cyber security exercises to validate and improve their plans, playbooks and technical capability to detect, respond to, and rapidly recover from a cyber incident.



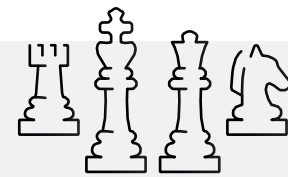
Methods and tools

The evolution of the cyber threat environment

Reporting is rising



A 36% increase in cyber security incidents reported to ASD's ACSC over the last five years.



State actors remain a significant threat

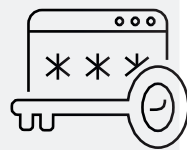
State actors continue to target Australian governments and businesses to conduct espionage and gain strategic advantage.

They may also be motivated to maintain options to disrupt essential services during periods of crisis or conflict.

Attackers steal access, not just data

The easiest way into a network is by using stolen or compromised legitimate credentials.

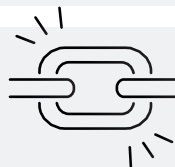
- Stolen usernames, passwords, tokens and sessions are now among the most common pathways into Australian networks.
- Identity fraud remained the most reported cybercrime for individuals over the last five years.
- Compromised accounts and credentials have become one of the top incident categories across government, industry and CI.



Data breaches have remained steady

- FY2021–22: 7% of all incidents
- FY2025–26: 6% of all incidents

Ransomware remains a persistent and disruptive threat



On average 11% of all incidents since FY2021–22 involved ransomware

- FY2021–22: 135 Ransomware incidents
- FY2025–26: 139 Ransomware incidents

Growing malicious use of AI



Advances in AI are lowering the barrier to entry for malicious cyber actors

- Enabling social engineering
- Creating highly convincing deep fakes and impersonations
- Writing and adapting malicious code faster
- Scanning and exploiting vulnerabilities at scale

A more professionalised cybercrime ecosystem

Cybercrime is a thriving industry



Specialised roles (e.g. developers and access brokers)



Cybercrime-as-a-Service (e.g. tools, kits and infrastructure for hire)



Efficient money laundering and monetisation networks



Active forums, markets and communities sharing knowledge and tools

While technologies and tactics will evolve, cyber resilience will remain Australia's strongest defence against an increasingly complex threat environment.

FIGURE 7: The evolution of the cyber threat environment

Analysing incidents using the MITRE ATT&CK framework

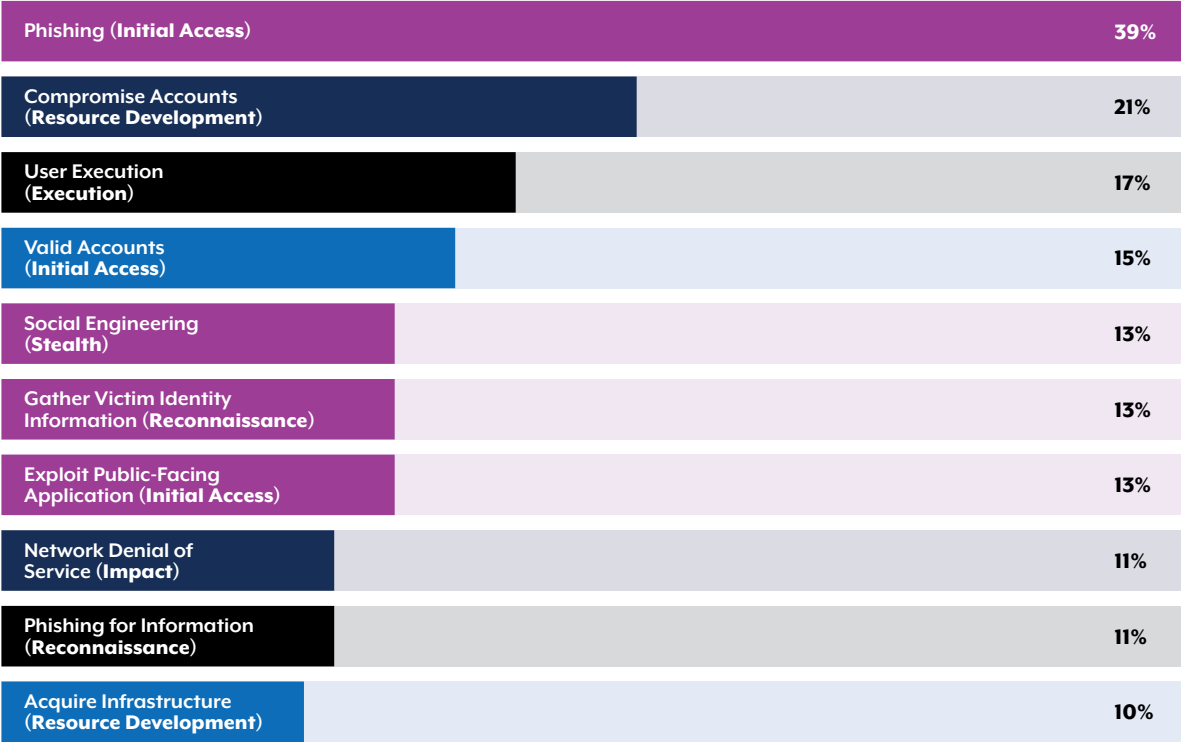


FIGURE 8: Prevalence of top 10 MITRE ATT&CK techniques in FY2025–26

ASD’s ACSC observed a range of common techniques malicious cyber actors used to exploit vulnerabilities in technology and systems, mapped against the MITRE ATT&CK framework.

During FY2025–26, there was a notable shift away from reconnaissance techniques and a move towards direct access and execution techniques. Phishing remained the most observed initial access technique, with entities specifically warned to beware of spearphishing links. Interestingly, gathering victim identity information decreased from 30% in FY2024–25 to 13% in FY2025–26.

Supply chains

Managing supply chain and third party risk should be a core component of any cyber security strategy. The cyber security risks of your suppliers and third parties are also your risks – you are only as strong as your weakest link.

Effective cyber supply chain risk management ensures, as much as possible, the secure supply of products and services throughout their lifetime. This includes their design, manufacture, delivery, maintenance, decommissioning and disposal. As such, cyber supply chain risk management forms a significant component of any organisation's overall cyber security strategy.

If products or services access valuable systems, operate with privileged access or have control over a large portion of a cyber supply chain, they may represent a weakness that could be exploited by malicious cyber actors. In such cases, this could have wide-reaching and harmful consequences.

CASE STUDY 4: AKIRA SONICWALL EXPLOITATION

In August 2025, numerous organisations across Australia reported to ASD's ACSC that they had been impacted by ransomware incidents. Thanks to proactive reporting from multiple organisations, ASD's ACSC was able to analyse the combined technical data and identify a known SonicWall vulnerability being actively exploited to gain unauthorised access and deploy ransomware. ASD's ACSC was then able to match the observed activity to the known tactics and behaviour of the Akira ransomware group, highlighting the potential scale and national impact.

ASD's ACSC conducted scans to identify potentially vulnerable organisations, identifying almost 1,000 potentially vulnerable devices and around 40 potentially vulnerable Australian organisations, many of them critical infrastructure entities.

ASD's ACSC proactively notified these potentially vulnerable organisations and published a public alert, providing Australian organisations with guidance issued by the vendor on how to protect their devices and remediate the vulnerability. Following the publication of the alert, ASD's ACSC observed a reduction in reported incidents using similar techniques against Australian organisations.

When organisations report incidents, vulnerabilities, and data such as Indicators of Compromise (IOCs) to ASD's ACSC, they help protect not only themselves but also the entire Australian community.

Code repositories

Since September 2025, ASD's ACSC has tracked the ongoing targeting of online code repositories (repos). Malicious cyber actors have been observed accessing online code repos through social engineering techniques, compromised credentials and authentication tokens. These malicious cyber actors then:

- abuse legitimate tooling and functions to modify public software packages to initiate supply chain compromises
- extract and publicly leak identified credentials publicly
- migrate private code repos to public code repos, and
- run open-source tools to scan for cryptographic secrets, passwords and sensitive keys stored in online code repos, rather than use bespoke tooling. Exposed code bases give malicious cyber actors a better understanding of internal processes and systems, increasing an organisation's attack surface and enabling future, novel attacks.

The compromise of trusted software packages presents an ongoing risk for organisations. These packages are often widely used and embedded as dependencies within other software, increasing the potential impact when vulnerabilities are identified.

To manage this risk effectively, organisations must be able to rapidly identify which software packages – and which specific versions – are installed across their environments. This information should be accurately collected, maintained and readily accessible. This enables organisations to quickly assess threat intelligence related to compromised software, determine its relevance to their environment, and take prompt action to reduce the risk of compromise.

CASE STUDY 5: GITHUB INFECTION

Since September 2025, ASD's ACSC has monitored a self-replicating malware (worm) known as 'Shai-Hulud', responsible for compromising hundreds of GitHub software packages.

After an initial compromise of a GitHub repo maintainer's account, malicious cyber actors published a malicious version of a widely used software package. This poisoned package cascaded through downstream dependencies, enabling rapid and wide-spread infection across the software supply chain.

The 'Shai-Hulud' malware was designed to harvest credentials and exfiltrate them to an actor-controlled endpoint. It would then programmatically create a new public GitHub repo named 'Shai-Hulud' under the victim's account and uploads the stolen secrets to it, publicly exposing them.

Using the stolen secrets, the malware can authenticate as the compromised developer, identify other packages maintained by that developer, inject malicious code, and publish the new compromised versions to the software registry. This automated process allows the malware to spread exponentially without direct intervention by the malicious cyber actor.

The 'Shai-Hulud' worm's self-replicating design is particularly notable, effectively combining credential harvesting with an automated dissemination mechanism that exploits developer account permissions to spread. This highlights the risks in today's interdependent software ecosystem and the importance of understanding and securing software supply chains.

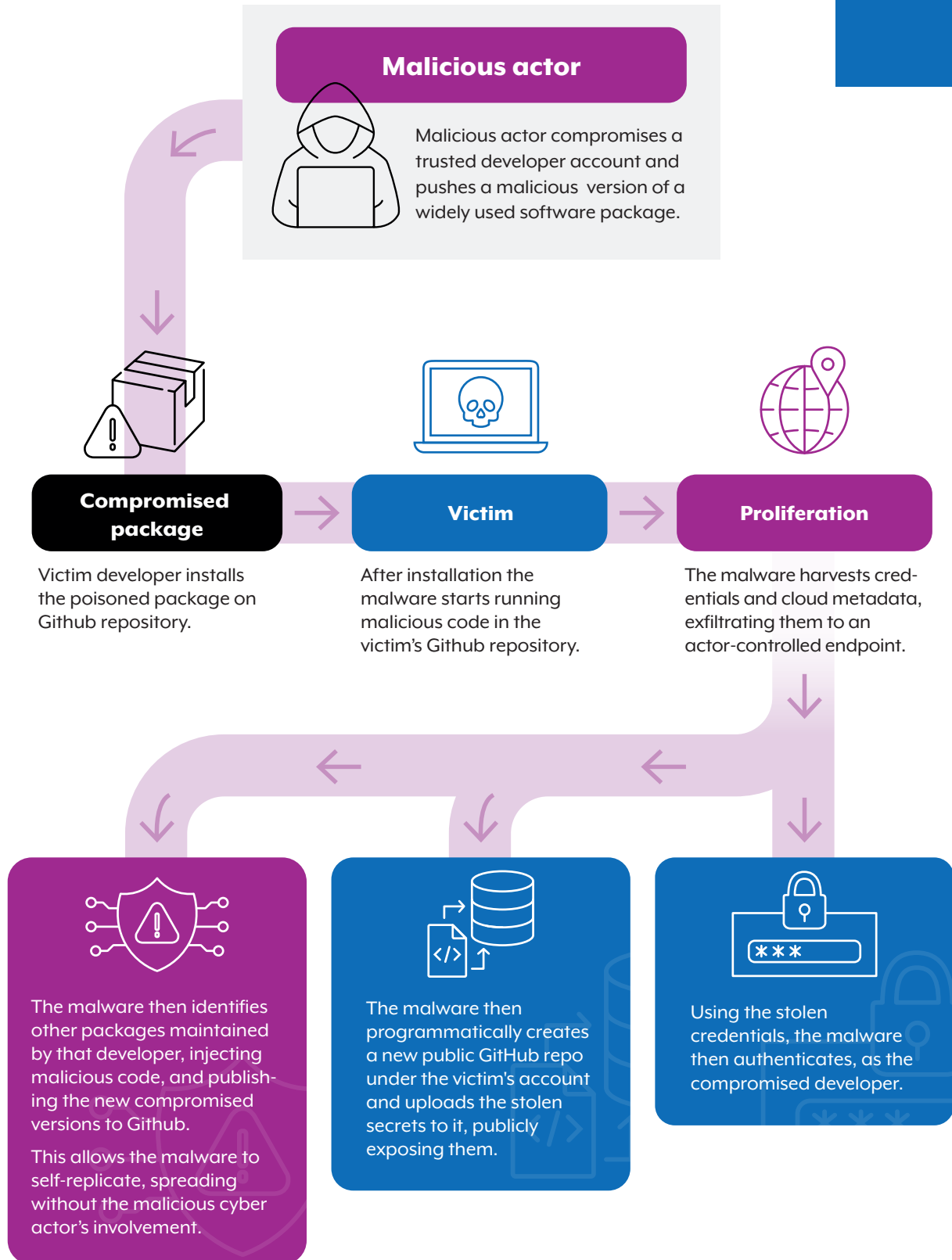


FIGURE 9: How malicious actors targeted online code repositories





Resilience

- AI is transforming the cyber security landscape by creating new opportunities to strengthen defences while also enabling cyber threats. Australian organisations must embrace AI to improve resilience while preparing to counter malicious uses of AI by adversaries.
- The question is no longer whether an organisation will face a cyber incident, but how prepared it is to respond. Building cyber resilience means maintaining critical operations and recovering quickly when incidents occur.
- Timely reporting of incidents to ASD's ACSC means we can provide specialist technical advice. Reporting improves situational awareness and protects other organisations from similar threats.
- Cyber resilience is a shared responsibility. Strong partnerships between government, industry and the community are essential to Australia's cyber security. In FY2025–26, ASD's ACSC's Cyber Security Partnership Program grew to over 149,500 partners. By participating in ASD's ACSC's partnership programs, organisations can access timely threat intelligence, share information, and strengthen collective resilience.

What you can do

Cyber Action Year: Awareness to Action

From the beginning of 2026, ASD's ACSC has brought leaders from across government, industry and CI together to be part of something bigger: a coordinated effort through the inaugural Cyber Action Year focused on delivering practical, measurable cyber security outcomes to counter a worsening threat environment.

ASD's ACSC is urging Australian industry to adopt the 'assumed breach' mindset, which takes a premediated planning approach for when, not if, a cyber compromise occurs. Five critical actions that every organisation should be working towards have formed the focus of Cyber Action Year:



Replace or mitigate legacy technologies



Prepare for post-quantum cryptography



Implement best practice event logging



Prepare for AI-enabled cyber threats

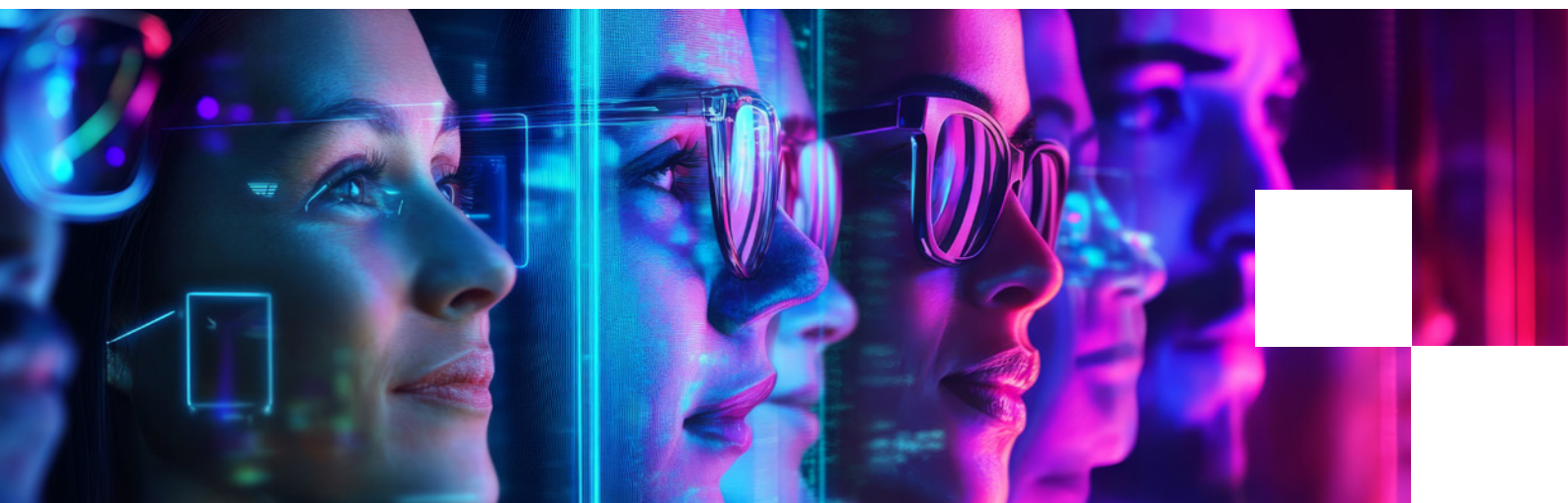


Supply chain management, including choosing secure by design

Importantly, these actions help organisations prepare for AI-enabled cyber threats as it enables malicious actors to identify vulnerabilities, develop exploits and conduct cyber operations more quickly and at greater scale. Reducing exposure to legacy technologies, improving visibility through event logging, adopting Secure by Design products and services, and preparing for PQC all strengthen an organisation's resilience.

Cyber Action Year is translating awareness into action. Organisations have shown a strong willingness to address cyber risks when presented with clear problems and actionable solutions, as demonstrated by the legacy technology uplift activities in March (for more information see Highlight 6: Addressing legacy technology risks through CHIPS).

As Cyber Action Year progresses, one lesson is clear: awareness alone is not enough. Most organisations understand cyber security risks, but turning awareness into meaningful action can be challenging amid competing priorities and an increasingly complex threat landscape. By providing clear, practical and actionable steps, ASD's ACSC is helping organisations move from knowing to doing, building momentum toward a more cyber secure Australia.



HIGHLIGHT 6: ADDRESSING LEGACY TECHNOLOGY RISKS THROUGH CHIPs

In March, Cyber Action Year focused on the risks posed by legacy technology and encouraged industry and government to uplift software versioning and identify, replace or mitigate legacy technology.

Legacy technology is outdated hardware and software that is no longer supported by the manufacturer, vendor or developer and cannot receive important security updates or patches. It presents significant and enduring risks to the cyber security posture of government and organisations. The most effective method to mitigate the risk posed by legacy tech is to replace it before it becomes unsupported.

To support the legacy technology focus, the Cyber Hygiene Improvement Program (CHIPs) expanded its service offering in February 2026 by introducing detection capabilities for 8 End-of-Life (EoL) products. Once identified, CHIPs sent reports to customers, recommending for each EoL product, that either they update it to a version that is in support, change to another product at a supported version, or decommission if the product was no longer needed.

Follow-up scans of customer systems revealed a significant reduction in products that were past EoL. From February to June, there was a 31.7% reduction in EoL products across all CHIPs customers.

Sector-specific results also demonstrated positive outcomes, with Commonwealth entities reducing EoL products by 31.7% and CI organisations achieving a 30.2% reduction over the same period.

CASE STUDY 6: RANSOMWARE AND THE IMPORTANCE OF EVENT LOGGING

In mid-2025, ASD's ACSC was engaged by an Australian organisation in response to a ransomware incident. The ransomware attack disrupted several building systems that were critical to the organisation's day-to-day operations, including security cameras, building access controls, lighting and lifts, and more than 30 virtual servers.

Fortunately, the organisation had comprehensive event logging in place, meaning that their operating system recorded key information about the malicious cyber incident, including:

- how the malicious cyber actor gained access
- which systems had been affected, and
- what actions the malicious cyber actor had taken.

The event logs also showed that the malicious cyber actors had not stolen any data from the organisation's network, which gave the organisation confidence that the incident, while disruptive, was limited in scope. Additionally, because the organisation had a practice of backing up their systems, essential services were restored promptly.

ASD's Essentials series

To ensure the continued effectiveness of ASD's mitigation advice in the changing threat environment, in October 2026 ASD's ACSC released the Essentials series. This is the evolution of ASD's Essential Eight into a broader, principles-based approach, offering prioritised, threat-informed cyber security mitigations with technology-specific content.

Originally released in 2017, and regularly updated, the Essential Eight was designed to provide guidance for enterprise IT networks. ASD's Essential Eight remains effective in preventing cyber security incidents, but the threat environment and technologies have evolved significantly since it was first developed.

The Essentials series was initially published with three chapters, each focused on a specific technology environment: Enterprise IT, Operational Technology and Cloud. The Essentials series helps organisations prioritise cyber security activities around their most important systems, services and data, while providing guidance that reflects the technologies they use.

Implementation of the Essential series framework will enable organisations to focus on the actions that will have the greatest impact on reducing cyber risks in their systems and better prepare Australian organisations to be resilient to current and future cyber threats.

ASD's ACSC acknowledges that organisations that have implemented the Essential Eight maturity model have made significant and valuable investments in their security posture. The evolved Essentials for enterprise IT framework does not discard that work. Indeed, this investment can be carried forward by organisations as part of implementing the Essentials. However, the mitigations and how we measure them have evolved and, in many cases, apply more broadly.

The development of the Essentials series was informed by ASD's unique intelligence insights, cyber security incident data, public cyber threat reporting, and consultation with partners across industry and government.

Throughout 2026, ASD's ACSC has engaged with industry and government partners through more than 30 face-to-face workshops across all 8 capital cities, a consultation paper released via ASD's Partner Portal, and bespoke targeted consultations for the cloud and operational technology chapters.

This process enabled implementers and service providers to shape the development of the Essentials series, while ensuring it is threat informed and supported by clear progression pathways and improved usability.

ASD's ACSC will continue to engage with stakeholders on the transitional arrangements into 2027.



Opportunities for resilience with and against AI

Rapid advancements in AI technologies over the past year are creating significant opportunities for businesses to strengthen cyber security, improve productivity and enhance resilience. While malicious actors are also adopting these technologies, AI has the potential to be a force multiplier for defenders, enabling organisations to identify threats earlier, respond faster and use cyber security resources effectively.

AI can help organisations improve cyber defence by automating repetitive tasks, analysing large volumes of security data at speed, and supporting more consistent and effective decision-making. For many businesses, particularly those with limited cyber security resources, AI-enabled tools can increase visibility of cyber risks and help security teams focus on higher-value activities.

Organisations that integrate AI tooling into their security operations can detect vulnerabilities earlier, improve software quality, monitor unusual behaviour, and respond faster to cyber incidents – reducing both the cost and impact of incidents.

AI can also support a range of defensive cyber security functions, including threat detection, vulnerability management, incident response, malware analysis and cyber threat intelligence. These capabilities can help organisations identify emerging threats more quickly, prioritise remediation efforts and improve overall cyber resilience. By reducing the time required to analyse information and investigate incidents, AI can help businesses operate more securely and efficiently.

Many AI use cases involve processing sensitive operational information. Businesses should use AI while maintaining appropriate controls and protecting information, in line with security and data handling obligations. This includes enforcing least privilege access, restricting data exposure to AI systems, validating outputs before use and maintaining auditability of AI-assisted actions.

Organisations must take steps to defend against AI-enabled threats, such as:

- Small businesses can reduce risk by choosing products that are Secure by Design out of the box, enabling automatic updates, and ensuring clear responsibility for security monitoring and incident response.
- Medium-sized businesses should maintain inventories of internet-facing systems, promptly patch vulnerabilities, implement network segmentation and test incident response and business continuity plans.
- Large enterprises, CI operators and government entities should establish executive accountability for AI-related cyber risks, adopt comprehensive monitoring and logging, and work towards layered Zero Trust and Secure by Design architectures supported by human-supervised defensive AI.
- Organisations should actively minimise their attack surface by ensuring only necessary systems and services are exposed to the internet, as AI-enabled exploitation is shrinking the window between vulnerability discovery and compromise.

Cyber resilience cannot be treated as a purely technical issue. It is a core business risk and leadership responsibility. As AI adoption continues to grow, organisations that effectively integrate AI into their cyber security practices will be better placed to manage risk, improve operational efficiency and respond to an increasingly complex threat environment. Organisations should continually assess the costs, benefits and risks of AI, recognising that both AI capabilities and their use by malicious actors will continue to evolve. Cyber risk assumptions can become outdated in months, not years. Success will depend on getting the fundamentals right, acting quickly and integrating cyber security into core business strategy. Organisations should also consider integrating AI into cyber security practices. For many organisations, AI represents not only a new area of risk, but a significant opportunity to build stronger, more adaptive and more resilient cyber defences.

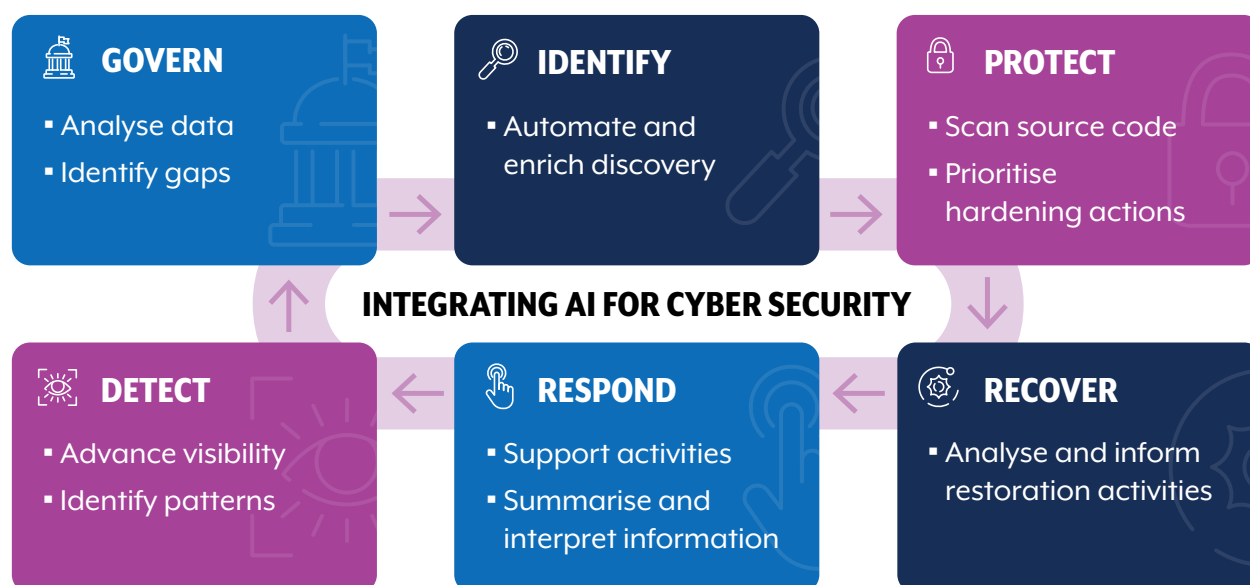


FIGURE 10: Applying AI across the six cyber security functions

Patching

Malicious cyber actors are moving quickly to exploit critical vulnerabilities, rapidly developing exploits to compromise networks. AI is shortening the time between vulnerability discovery and exploitation. ASD's ACSC recommends that all entities accelerate their patching process and prioritise security updates accordingly to manage risks.

Having clear and streamlined patch management helps organisations respond quickly to new vulnerabilities. By understanding vendor patch schedules and regularly scanning for missing patches, organisations can dramatically reduce the time between identifying new vulnerabilities and applying fixes.

Preparing for post-quantum cryptography

Cryptographically relevant quantum computers (CRQCs) are being accelerated as recent research and development becomes reality, requiring Australia to prepare for Q-day, the point where a CRQC is able to break standard public-key cryptography.

The creation of CRQCs presents new cyber security risks as adversaries may use CRQC capabilities to threaten the security of current systems that rely on traditional asymmetric cryptographic algorithms.

PQC provides a solution by using quantum-resistant algorithms designed to remain secure against future quantum computing threats. Organisations should address the threat of CRQCs and prepare to protect their IT environment now. Some service providers and vendors have begun transitioning to PQC, with some offering PQC-only solutions and products, highlighting the need for organisations to start planning their PQC transition sooner rather than later.

ASD's ACSC recommends ceasing the use of traditional asymmetric cryptography and transitioning to PQC by the end of 2030, or sooner, which will ensure organisations are at lower risk should AI speed up developments in quantum computing. Organisations will need to consider multiple factors when planning their PQC transition, as successful transition across different organisations may vary. Factors could include the scale of IT environments, the nature of the cyber threats faced, the availability of resources, or any need to maintain interoperability with legacy systems used by business partners and customers.

ASD's ACSC encourages organisations to consider the LATICE framework, when undertaking their PQC transition: locate, assess, triage, implement, communicate and educate.

For more information, visit ASD's ACSC quantum-related publications on cyber.gov.au/quantum.

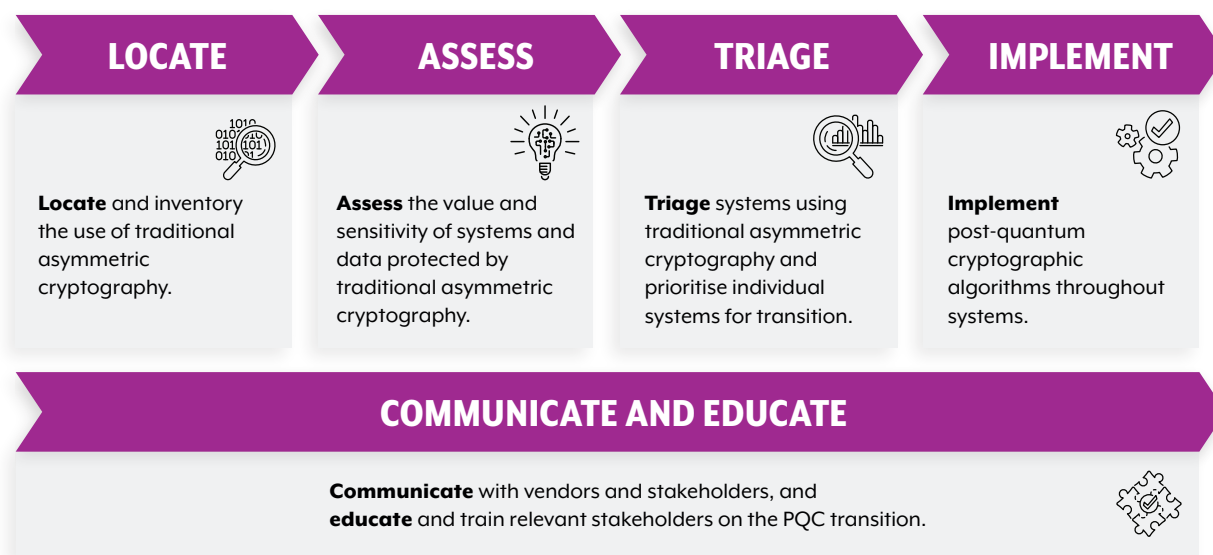


FIGURE 11: LATICE framework

Small and medium-sized organisations – including those operating bespoke, regulated, on-premises or critical systems – cannot easily transition to PQC across complex IT environments. However, they do not need a massive budget or a large security team to begin addressing quantum risk. Where possible, organisations should look to adopt PQC by implementing solutions that are post-quantum ready, doing it in-house, or through new or existing service providers who can provide vendor-managed updates to websites, cloud services and software.

Preparing for service disruption or crisis

OT systems are particularly vulnerable to cyber attacks. Many were never designed to withstand cyber threats and are now exposed to adversaries with sophisticated capabilities.

In October 2025, ASD's ACSC released CI Fortify. The series provides practical, principles-based guidance to help CI withstand cyber threats and recover quickly in the event of an incident, ensuring the continuity of critical services during crises or prolonged disruptions. CI Fortify should be prioritised by all Australian CI operators.

To achieve this capability, organisations should:

- identify vital OT and enabling systems that support a critical service as well as associated isolation points
- develop the capability to physically isolate vital OT and enabling systems from the internet and other networks for three months while continuing to maintain critical services
- be able to rapidly and fully rebuild vital OT and enabling systems to minimise disruption to critical services.

ASD's ACSC's latest publication in the series, *Advice for Isolating Vital Systems*, provides guidance to OT system owners and operators, and cyber defenders in adopting CI Fortify's physical isolation requirement. The physical isolation of vital systems removes operational independence between OT and IT networks, enabling continued delivery of critical services even if corporate networks become inoperable or degraded.

The ability to fully rebuild isolated OT and supporting systems is equally critical, allowing for effective incident response and the safe, timely restoration of services. This is particularly important where malicious activity may persist beyond the temporary isolation period, or where initial recovery efforts prove unsuccessful.

Report cyber security incidents to ASD's ACSC

Australian organisations that have been, or may have been, impacted by a cyber security incident are encouraged to reach out to ASD's ACSC. ASD's ACSC offers free technical incident response advice and assistance, 24 hours a day, 7 days a week.

We also recommend responding to ASD's ACSC when we reach out to you regarding a vulnerability, potential compromise or a confirmed compromise that could impact your organisation. If you are concerned about the legitimacy of a call, you can verify that you were speaking to a genuine representative of ASD's ACSC by calling **1300 CYBER1** (1300 292 371) and quoting your incident/reference number.

Report a cybercrime or cyber security incident

Report at

cyber.gov.au/report

or call the 24/7 Australian Cyber Security Hotline on

1300 CYBER1 (1300 292 371)

Cybercrime reports are automatically referred to the relevant state or territory law enforcement agency. An incident does not have to be a confirmed compromise to be reported and could include:

- DoS
- scanning and reconnaissance
- unauthorised access to a network or device
- data exposure, theft or leak
- malicious code/malware
- ransomware
- a vulnerability
- phishing/spearphishing
- any other irregular cyber activity that causes concern.

How ASD's ACSC can help

When you report, ASD's ACSC will provide immediate incident response advice and assistance, which may include:

- providing information on how to contain and remediate the cyber security incident
- providing advisory products to assist you with your incident response
- linking you to Australian government organisations that may further support your response
- triaging the incident to determine if there are more detailed actions to be undertaken
- assessing whether the incident requires a more tailored approach, and, depending on the incident, we may offer:
 - a team of digital forensics specialists to support a comprehensive technical investigation
 - guidance on approaching public communications to ensure transparency while protecting the integrity of the technical investigation
 - information and reports to help you finalise your investigation
 - an introduction to different areas within ASD's ACSC for additional support, such as cyber resilience uplift activities and, if requested, help you to contact the Department of Home Affairs or the AFP.

How your reporting matters

ASD's ACSC uses anonymised information from your report to build our understanding of the cyber threat environment. This understanding assists with the development of new and updated advice, capabilities, techniques and products to better prevent and respond to evolving cyber threats.

Reporting an incident could be the key to preventing further victims.

Your confidentiality is paramount

ASD's ACSC is not a regulator and does not share any information provided by you without your express consent. We are then legally bound to use your information for cyber security purposes only, to better assist you and protect the Australian community. Your confidentiality is further protected under ASD's ACSC's 'limited use' obligation.

Programs

Partnership and collaboration with ASD's ACSC

ASD's ACSC works closely with government and private enterprises to identify and disrupt malicious cyber activity and helps entities improve their cyber defence through a range of programs.

In FY2025–26, ASD's Cyber Security Partnership Program grew to over 149,500 partners. ASD's ACSC briefed board and executive leadership team representatives from 29% of the ASX100.

ASD's Cyber Security Partnership Program is a national program delivered through ASD's state offices, located around Australia. The program enables eligible Australian organisations to engage with ASD's ACSC and industry and government partners, drawing on collective understanding, experiences, skills and capabilities to enhance understanding of the cyber threat, and uplift cyber resilience across the Australian economy.

The Cyber Hygiene Improvement Programs (CHIPs) is an open-source intelligence capability that discovers, identifies and regularly measures the cyber posture and hygiene of internet-facing systems, using objective and data-driven approaches. The program relies on a mixture of open-source, commercial and directly collected data.

CHIPs helps to improve cyber hygiene, particularly in attack surface reduction, by providing entities with regular reports that identify the extent of their internet-facing systems as well as any identified weaknesses or vulnerabilities in those systems.

CHIPs also responds to critical vulnerabilities and other significant cyber events, providing entities with timely, actionable intelligence to help them protect themselves in rapidly changing situations.

The Critical Infrastructure Uplift Program (CI-UP) assists Australian CI organisations to improve their resilience against cyber attacks, with a focus on hardening against attack pathways to CI assets and OT environments. A voluntary, nationwide threat-driven program, CI-UP focuses on improving CIs cyber security in a range of areas, including:

- enhancing visibility of malicious cyber activity and awareness of vulnerabilities
- enhancing the ability to contain and respond to an incident
- furthering a cyber security culture.

CI-UP leads this work through a series of programs that share uplift and hardening advice and provide technical assistance. These include:

- **1:1 Uplift activities** – invitation-only activities focused on uplifting the cyber security of CI assets most important to Australia's national security.
- **Sprint Uplift activities** – invitation-only cyber uplift engagements delivering rapid uplift services to a broad cross-section of Australian CI.
- **Operational Technology Information Exchanges (OT-IEs)** – forums for ASD's ACSC partners in CI sectors with OT capability to discuss the OT cyber threat landscape in a neutral and trusted environment.
- **CI-UP presentations, briefings and workshops** – provide sector-specific insights and trends across a range of CI partners.

The Government Uplift Program assists prioritised government entities to strengthen their cyber resilience. The program provides technical assessment and remediation based on current and emerging threats, as well as training, engagement and guidance for those in critical IT and management roles within government. The program of work includes:

- **Government Cyber Assessment Team (GovCAT)** – a threat-led and hands-on technical assessment of priority entity environments and systems that provides actionable insights for immediate cyber security uplift.
- **The Cyber Uplift Remediation Program (CURP)** – hands-on technical implementation and remediation activities with prioritised government entities to uplift their cyber security resilience.
- **Training and support** – for cyber security staff across government. This includes targeted training for 9,955 privileged users as well as uplifting the skills of 93 cyber defenders responsible for cyber visibility.
- **Engagement and guidance** – supporting both executives and cyber technical practitioners with situational awareness, threat assessments, specialised tools, and technical assistance.
- **Targeted projects** – seeking to measure and improve priority government web apps, improve the configuration of commonly used products and test new models of cyber defence and visibility across government.

Threat sharing and threat blocking is a key initiative under the *2023-2030 Australian Cyber Security Strategy: Shield 3 - World Class Threat Sharing and Blocking*.

ASD's ACSC has continued its partnership with the Department of Home Affairs to align its existing bodies of work on threat sharing and blocking, working to enhance ASD's ACSC's capabilities by providing the backbone of the Threat Blocking and Threat Sharing Scheme.

ASD's ACSC is enhancing the ability of banks and telecommunication providers to share IOCs with actionable intelligence, blocking cyber threats with precision, speed, and scale.

HIGHLIGHT 7: DISRUPTING THE HelloTDS MALICIOUS REDIRECTION CAMPAIGN

ASD's ACSC analysts successfully identified and mitigated a large-scale malicious traffic redirection campaign impacting Australian organisations known as HelloTDS, demonstrating the value of proactive threat intelligence sharing and collaboration.

During the investigation, analysts uncovered extensive infrastructure consisting of over 20,000 Traffic Direction System (TDS) domains. These domains were cleverly designed to funnel users who had clicked on an advertisement toward a relatively small set of 30 malicious command domains, enabling malicious actors to efficiently manage and scale their operations while evading detection.

ASD's ACSC played a critical role in disrupting the campaign by:

- sharing the full list of malicious domains, infrastructure, and IOCs with partners via ASD's ACSC CTIS
- blocking malicious domains via Australian Protective Domain Name System (AUPDNS)
- issuing domain take downs to remove the malicious domains via ASD's ACSC's takedown service.

This coordinated response resulted in the rapid containment and disruption of the campaign's infrastructure, reducing exposure and limiting the potential compromise of Australian organisations. It also armed ASD's ACSC partners to defend their own networks.

HIGHLIGHT 8: DISRUPTING A BEC IMPERSONATION CAMPAIGN

In December 2025, ASD's ACSC identified a large-scale Business Email Compromise (BEC) campaign after receiving reports of domains impersonating Australian construction companies. Further analysis revealed over 400 look-alike domains being used to send fraudulent emails.

Unlike traditional BEC attacks, this campaign did not involve compromised accounts. Instead, attackers used look-alike domains and email infrastructure to impersonate trusted businesses and trick victims into making urgent payments.

ASD's ACSC responded by:

- sharing 423 confirmed malicious domains via CTIS block feeds
- providing cyber threat intelligence to help partners proactively defend their networks.

ASD's ACSC identified many domains in this campaign that were staged for malicious activity but were not yet active. Sharing these with partners and blocking them via AUPDNS enabled ASD's ACSC to disrupt the threat before widespread impact.

HIGHLIGHT 9: CLICKFIX ATTACK VECTOR DISRUPTION

ASD's ACSC identified the ClickFix attack vector that targeted Australian networks by injecting malicious domains into websites that belonged to legitimate Australian businesses. The ClickFix attack vector tricked users into executing malicious commands delivering malware via deceptive verification prompts like fake CAPTCHAs (Completely Automated Public Turing test to tell Computers and Humans Apart).

ASD's ACSC responded by:

- advising Australian businesses of their website compromises
- sharing 125 IOCs via CTIS
- blocking the malicious domains on AUPDNS
- disseminating a public cyber advisory.

The sharing of the ClickFix attack vector via CTIS and public advisory has limited its effectiveness and helped Australian organisations, from governments to small businesses, to protect their own networks.

Notes

Sources

ASD's ACSC manages or uses several unique datasets to produce tailored advice and assistance for Australian organisations and individuals. Not all cybercrimes lead to cyber security incidents, and the statistics in this report are from 2 distinct datasets: cybercrimes reported to law enforcement through ReportCyber, and cyber security incidents responded to by ASD's ACSC. Data has been extracted from live datasets of cybercrime and cyber security reports disclosed to ASD's ACSC. The self-reported ReportCyber statistics used throughout this Annual Cyber Threat Report serve as a guide to indicate cyber threats that individuals and organisations are currently experiencing. As such, the statistics and conclusions in this report are based on point-in-time analysis and assessment. Cybercrime and cyber security incidents reported to ASD's ACSC will not reflect all cyber threats and trends in Australia's cyber security environment.

ASD's ACSC encourages the reporting of cybercrimes, cyber security incidents and vulnerabilities to inform ASD's ACSC advice and assistance and enhance situational awareness of the national cyber threat environment.

Percentage changes of less than 5% are considered to represent a similar or consistent trend. Accordingly, such variations may not be specifically highlighted within this report.

Glossary

ASD's ACSC glossary provides definitions for terms used in this report and other ASD ACSC publications: see <https://www.cyber.gov.au/learn-basics/view-resources/glossary>.

AI use disclaimer

Artificial Intelligence tools were used sparingly throughout the production of this report. All AI-assisted outputs were reviewed by human contributors to ensure accuracy, appropriateness, and alignment with ethical standards.





cyber.gov.au