Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Annual Cyber Threat Report

2024–2025

Website

www.cyber.gov.au

Contact us

ASD's ACSC welcomes feedback to improve the services it provides to Australians.
Feedback can be provided by emailing asd.assist@defence.gov.au. Alternatively, a feedback form can be found at: https://www.cyber.gov.au/about-us/about-acsc/contact-us.

Copyright

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. We also recognise Australia's First Peoples' enduring contribution to Australia's national security.

Annual Cyber Threat Report

2024–2025

Foreword

I am pleased to present the Annual Cyber Threat Report 2024–25.

The world continues to face complex strategic circumstances. Competition and military build-up in the Indo-Pacific, and ongoing global conflicts are challenging Australia's security and the global rules that have endured since World War II. In this uncertain environment, Australia's relationships with friends and allies are more critical than ever.

Over the past year, we continued to see state-sponsored cyber actors targeting Australian networks to steal sensitive information.

Australia joined multi-country advisories warning of the threat of state-sponsored actors targeting critical infrastructure for the purposes of positioning for potential disruptive attacks. One such advisory details how People's Republic of China-affiliated threat actors targeted the networks of major global telecommunications providers to conduct a broad and significant cyber espionage campaign. Another details a Russian state-sponsored cyber campaign targeting Western logistics and technology businesses. I urge Australian businesses to review and apply the ASD and its partners' technical advice to protect your networks.

Cybercriminals also relentlessly targeted Australians, with ransomware attacks and data breaches increasing in frequency. Using malware designed to covertly harvest information from Australian victims, cyber criminals used stolen data, usernames and passwords to launch subsequent attacks, compromise corporate networks and accounts.

The Australian Government continues to invest in the nation's cyber capabilities through project REDSPICE, which doubles ASD's size and ability to strike back against malicious cyber activity. In February 2025, the Australian Government imposed cyber sanctions on a Russian business and its employees for storing and facilitating the theft of millions of incredibly personal digital records posted by cybercriminals on the darkest corners of the internet. The sanctions were preceded and enabled by ASD's targeted offensive cyber activity which disrupted criminal infrastructure used to host stolen personally identifiable information (PII) of millions of victims around the world.

This was the first time Australia imposed cyber sanctions on an entity responsible for providing the infrastructure facilitating cybercrime. It was made possible by ASD's hard work and delivered in collaboration with domestic and international industry, intelligence and law-enforcement partners.

This report outlines the cyber threats the nation is facing. All Australians have a role in taking action to increase Australia's cyber resilience.

The Hon Richard Marles MP
Deputy Prime Minister and Minister for Defence

Contents

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 contactable 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 between over 133,000 Australian organisations and individuals on cyber security issues through ASD's 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

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 (JPC3) 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.

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 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.

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.

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*.

National Cyber Security Coordinator

The National Cyber Security Coordinator, supported by the National Office of Cyber Security (NOCS), 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*.

Australian Competition and Consumer Commission

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.

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.

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.

Executive summary

Australia is an early and substantial adopter of digital technology which drives public services, productivity and innovation. Our increasing dependency on digital and internet-connected technology means Australia remains an attractive target for criminal and state-sponsored cyber actors.

In FY2024–25, ASD's ACSC received over 42,500 calls to the Australian Cyber Security Hotline, a 16% increase from the previous year. ASD's ACSC also responded to over 1,200 cyber security incidents, an 11% increase. During FY2024–25, ASD's ACSC notified entities more than 1,700 times of potentially malicious cyber activity – an 83% increase from last year – highlighting the ongoing need for vigilance and action to mitigate against persistent threats.

State-sponsored cyber actors continue to pose a serious and growing threat to our nation. They target networks operated by Australian governments, critical infrastructure (CI) and businesses for state goals. State-sponsored cyber actors may also seek to use cyber operations to degrade and disrupt Australia's critical services and undermine our ability to communicate at a time of strategic advantage.

The threat from cybercrime also continues to challenge Australia's economic and social prosperity, with average reported financial losses, the frequency of ransomware attacks and the number of reported data breaches all increasing throughout FY2024–25. Cybercriminals are continuing their aggressive campaign of credential theft, purchasing stolen usernames and passwords from the dark web to access personal email, social media or financial accounts.

Malicious cyber actors are able to leverage vulnerabilities in the technology and security practices of individuals and businesses throughout the public and private sectors. Internet-facing vulnerabilities in edge devices are common, and they require network owners to rigorously monitor and configure securely. 'Living off the land' tradecraft has persevered, requiring an adjustment in the way network defenders prioritise understanding behavioural patterns of networks in order to detect the most sophisticated threats.

The prevalence of artificial intelligence (AI) almost certainly enables malicious cyber actors to execute attacks on a larger scale and at a faster rate. The potential opportunities open to malicious cyber actors continue to grow in line with Australia's increasing uptake of – and reliance on – internet-connected technology.

CI is, and will continue to be, an attractive target for state-sponsored cyber actors, cybercriminals, and hacktivists, largely due to large sensitive data holdings and the critical services that support Australia's economy. ASD's ACSC notified CI entities of potential malicious cyber activity impacting their networks over 190 times in the last reporting period – up 111% from the previous year.

The threat environment combined with our operational observations set out in this report underscores the need for all Australian individuals, private and public entities to take action to uplift our cyber resilience at every level. Every individual can uplift their cyber defences through basic actions. Use strong Multi-Factor Authentication (MFA) wherever possible, use strong and unique passwords or passphrases, keep software on devices updated, be alert for phishing messages and scams, and regularly back up important data. These basics have never been more important, and implementing these mitigations can prevent the majority of the cyber incidents reported to ASD's ACSC.

Businesses should operate with a mindset of 'assume compromise' and prioritise the assets or 'crown jewels' that need the most protection. ASD recommends businesses and network owners focus on 4 'big moves' to bolster their cyber defences and prepare for future challenges: implement best-practice logging, replace legacy IT, effectively manage third-party risk and prepare for post-quantum cryptography.

For those businesses also operating operational technology (OT), follow best-practice guidance for isolating vital OT and enabling systems, and have a plan for how to rebuild.

For large organisations, ensuring technology used or provided to customers is secure-by-design and secure-by-default is critical for building modern networks that protect data and systems.

The years ahead will bring challenges for organisations in emerging technology, such as post-quantum cryptography. ASD's ACSC will continue to work with Australian industry and partner organisations to ensure the continued security of our communications and sensitive data. Effective transition plans will be critical to operating in 2030 and beyond – a post-quantum computing world – and this planning must start now.

Businesses must ensure that, in order to harness the full benefits and productivity associated with AI, a safe and secure approach is taken to the integration of AI technologies.

It remains critically important that organisations and individuals who observe suspicious cyber activity, incidents and vulnerabilities report to ReportCyber at 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 **42,500** calls to the Australian Cyber Security Hotline, **up 16%**

- On average, **116 calls per day**, an increase from **100 calls per day**

Received over **84,700** cybercrime reports to ReportCyber, **down 3%**

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

Average self-reported cost of cybercrime per report for individuals, **up 8%** ($33,000)

Average self-reported cost of cybercrime per report for businesses, **up 50%** overall ($80,850)

- small business: **$56,600** (up 14%)
- medium business: **$97,200** (up 55%)
- large business: **$202,700** (up 219%)

Publicly reported common vulnerabilities and exposures **increased 28%**

11% of all incidents responded to included **ransomware**, *consistent with last year*

Responded to more than 200 incidents involving **Denial of Service** (DoS) or **Distributed Denial of Service** (DDoS), **up more than 280%** from last year

Identity fraud remained the top reported cybercrime, **up 8%**

YEAR IN REVIEW

What ASD's ACSC did

Responded to over **1,200 cyber security incidents**, an **11% increase** from last year

Notified entities of **potential malicious cyber activity** more than 1,700 times, **up 83%**

Australian Protective Domain Name System blocked customer access to **334 million** malicious domains, **up 307%**

Cyber Threat Intelligence Sharing (CTIS) partners grew by 13% to over **450 partners**

- In late 2024, CTIS transitioned to ASD's new enhanced CTIS platform
- To date, CTIS has shared over **2,984,000 indicators of compromise**

Cyber Hygiene Improvement Programs

- Performed **478** high-priority operational taskings, **up 31%**
- Distributed around **14,400** reports to approximately **3,900** organisations, **up 125%** and **95%** respectively
- Distributed around **11,000** Notifications of Indicators of Compromise to approximately **2,160** organisations

Government Uplift Program

- **26** active Cyber Uplift Remediation Program engagements (commenced prior to FY2024–25)
- **4** Cyber Uplift Remediation Program engagements commenced (during the reporting period)
- **7** active Cyber Maturity Measurement Program engagements

YEAR IN REVIEW

What ASD's ACSC did

Critical Infrastructure Uplift Program

- **8** CI uplifts completed, covering **38 CI assets**
- **4** CI uplift sprints completed, covering **5 CI assets**
  - With a further 2 CI uplift sprints in progress
- **7** Tech-To-Tech workshops held

Notified critical infrastructure entities of potential malicious cyber activity over **190 times, up 111%**

Published or updated **26 PROTECT** publications, including guidance publications related to the ***Essential Eight Maturity Model*** and updates to the ***Information Security Manual***

Published a combination of **108 alerts, advisories, knowledge articles and publications** on both **cyber.gov.au** and the **Partner Portal**

ASD's Cyber Security Partnership Program grew by 11% to over 133,000 partners

Led **17 cyber security exercises**, involving over **120 organisations**, to strengthen Australia's resilience

Briefed board and executive leadership team representatives from **41% of the ASX100**

YEAR IN REVIEW

July 2024

9 July jointly published *APT40 Advisory: PRC MSS tradecraft in action*

16 July updated *Hardening Microsoft Windows 10 and Windows 11 workstations* advice

30 July published *Secure–by–Design Foundations* to help technology manufacturers and consumers adopt secure-by-design principles

August 2024

22 August jointly published *Best practices for event logging and threat detection* to improve the security of critical systems

September 2024

2 September released advisory *The silent heist: cybercriminals use information stealer malware to compromise corporate networks*

6 September released joint advisory *Russian Military Cyber Actors Target U.S. and Global Critical Infrastructure*

19 September released joint advisory on *People's Republic of China-Linked Actors Compromise Routers and IoT Devices for Botnet Operations*

26 September jointly published *Detecting and mitigating Active Directory compromises*

October 2024

1 October Cyber Security Awareness Month 2024

2 October the Australian Government enacted cyber sanctions against prolific cybercriminal syndicate members of Evil Corp

2 October published *Principles of operational technology cyber security*, which was co-designed with Australian critical infrastructure operators

17 October released joint advisory *Iranian cyber actors' brute force and credential access activity compromises critical infrastructure*

25 October jointly published *Safe Software Deployment*

November 2024

21 November published updates to *#StopRansomware: BianLian Ransomware Group advisory*

29 November *Intelligence Services and Other Legislation Amendment (Cyber Security) Act 2024* became law

December 2024

4 December released joint advisory *Enhanced visibility and hardening guidance for communications infrastructure* in response to People's Republic of China (PRC)-affiliated cyber actors' exploitation of networks of major global telecommunication providers

January 2025

14 January jointly published *Secure by Demand: Priority considerations for operational technology owners and operators when selecting digital products*

22 January published *"Bulletproof" hosting providers: Cracks in the armour of cybercriminal infrastructure*

February 2025

5 February jointly published a series on securing edge devices

10 February published *Foundations for modern defensible architecture*, which introduces modern defensible architecture as an approach for building cyber resilience

12 February the Australian Government enacted further cyber sanctions against Russian cyber criminals including Australia's first sanction against a cyber infrastructure entity

March 2025

17 March released an advisory and joint guidance in response to increasing denial-of-service (DoS) attacks

18 March released significant updates to *ASD's Blueprint for Secure Cloud (the Blueprint)*

April 2025

4 April released joint advisory on the ongoing threat of fast flux-enabled malicious activities as a defensive gap in many networks

9 April released a joint advisory on 2 spyware variants, BADBAZAAR and MOONSHINE targeting Uygur, Taiwanese and Tibetan groups and civil society actors

May 2025

22 May released a joint advisory on the Russian targeting of Western logistics entities and technology companies

23 May released a joint advisory on best practices for securing data throughout the Artificial Intelligence (AI) system life cycle

28 May jointly published a suite of guidance to assist organisations implement Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) platforms

June 2025

5 June released an updated joint advisory on the Play ('Playcrypt') ransomware group's indicators of compromise (IOCs) and tactics, techniques and procedures (TTPs)

30 June published *Introduction to Connected Vehicles* as a foundational explainer on the technology and cyber security vulnerabilities of Connected Vehicles.

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.

	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
Sustained disruption of essential systems and associated services	C6	C5	C4	C3	C1	C1
Extensive compromise	C6	C5 7	C4 10	C3 7	C2 2	C1
Isolated compromise	C6	C5 52	C5 79	C3 51	C3 28	C2
Coordinated low-level malicious attack	C6 1	C6	C5 2	C4 2	C3 3	C3 1
Low-level malicious attack	C6 1	C6 128	C5 65	C4 109	C4 94	C3 9
Unsuccessful low-level malicious attack	C6	C6 33	C6 12	C6 183	C6 334	C6 40

Figure 1: Cyber security incidents by severity category for FY2024–25 (total 1,253)

Overall, there was an 11% increase in incidents reported to ASD's ACSC in FY2024–25. Compared to FY2023–24, there was a notable increase in successful and unsuccessful low-level malicious attacks. While the raw number of high-end attacks is lower this year, ASD nevertheless continued to see the use of complex and sophisticated tradecraft.

Incidents categorised as C3 or above involved organisations such as federal and state governments, large organisations, academia and supply chains. ASD's ACSC responded to 2 C2 incidents in FY2024–25, up from one in FY2023–24. C3 incidents in FY2024–25 were less frequent than in FY2023–24, with 8% of all incidents being categorised C3, down 6%.

Over a third (37%) of all C3 incidents were discovered as a result of ASD's ACSC proactively notifying the affected organisation of suspicious activity, an increase of 26%. C3 incidents commonly involved compromised assets, network or infrastructure (50%), compromised accounts or credentials (42%), and ransomware (34%). This contrasts with C3 incidents in FY2023–24, where accounts were more frequently compromised than assets, networks or infrastructure.

Caveat: Incidents can have multiple incident types ascribed to them and hence do not add up to 100%.

ASD's ACSC responded to **over 1,200 cyber security incidents**, an 11% increase from last year.

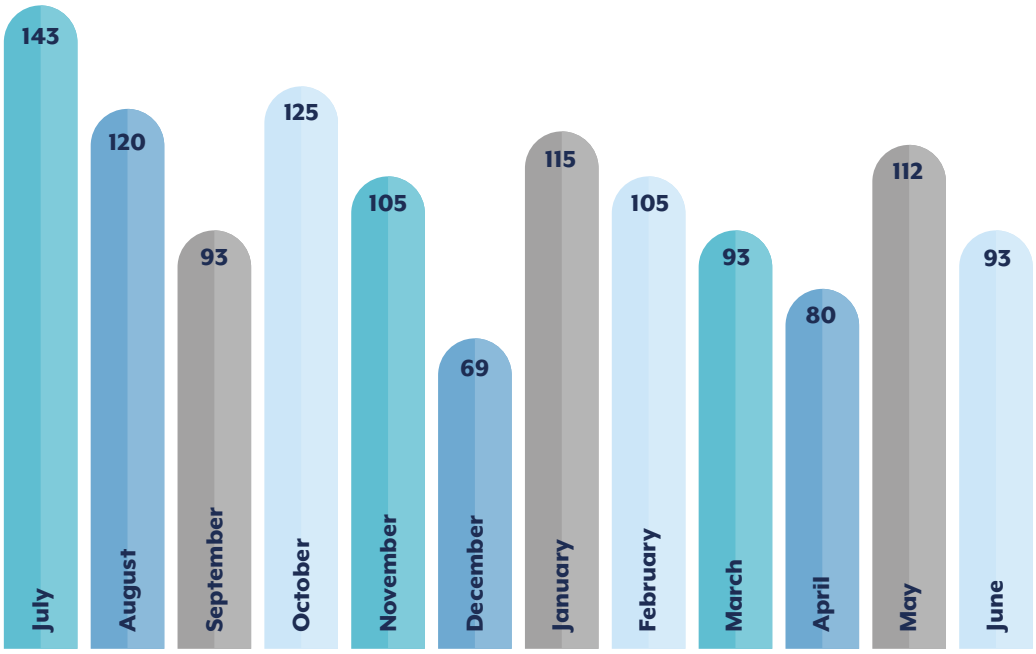


Figure 2: Cyber security incidents responded to by month

Reported top 3

Top 3 reported **cyber security incident** types for **critical infrastructure**

- Compromised Asset/Network/Infrastructure **55%**
- DoS/DDoS **23%**
- Compromised Account/Credentials **19%**

Top 3 reported **cyber security incident** types for **government** (federal, state and local)

- Compromised Asset/Network/Infrastructure **37%**
- DoS/DDoS **16%**
- Malware Infection (other than ransomware) **15%**

Top 3 self-reported **cybercrime** threats for **business** (Small, Medium, Large)

- Email compromise resulting in no financial loss **19%**
- Business email compromise (BEC) fraud resulting in financial loss **15%**
- Identity fraud **11%**

Top 3 self-reported **cybercrime** threats for **individuals**

- Identity fraud **30%**
- Online shopping fraud **13%**
- Online banking fraud **10%**

Note: Incidents can have multiple incident types.

Chapter 1

Australian cyber threat landscape

Who is **targeting Australia**

- Australia's economy and geostrategic position make it an attractive target for various malicious cyber actors.
- State-sponsored cyber actors are a persistent threat. They target a range of sectors to conduct espionage against both individuals and organisations, and to generate opportunities to disrupt critical services and communication at a time of strategic advantage.
- Cybercriminals target Australia's economy for financial gain. This can manifest in the theft of data or the disruption of services to elicit payment.

State-sponsored cyber actors

Over FY2024–25, state-sponsored cyber actors targeted Australian networks, and they continue to present an active and evolving cyber threat to Australia. State-sponsored cyber actors conduct operations to serve political and military objectives, including cyber espionage, malign influence, interference and coercion, or to pre-position for disruptive and destructive cyber effects in the event of crisis or conflict.

State-sponsored cyber actors routinely target Australian government networks for cyber espionage purposes. Government and defence-related information is an attractive target for state-sponsored cyber actors seeking strategic insights into Australia's national policies and decision-making.

However, government networks are not the only source of this information. Many Australian businesses and other organisations hold large amounts of sensitive and valuable data, such as proprietary information, research and personal data. State-sponsored cyber actors may use this data to support further targeting against government and critical infrastructure (CI) organisations, as well as their supply chains.

State-sponsored cyber actors have also compromised home devices connected to the internet, such as home routers, to create botnets that support further targeting around the globe.

State-sponsored cyber actors continue to use built-in network administration tools to carry out their objectives and evade detection by blending in with normal system and network activities, enabling them to decide when to steal information or cause harm to an organisation's network at a time of their own choosing. This is known as living off the land (LOTL). LOTL tradecraft requires network defenders to think like the malicious cyber actor, by studying abnormalities in behaviours occurring on systems rather than through traditional means such as intrusion detection systems.

State-sponsored cyber actors often use data from previous data breaches or cyber security incidents, such as network information and valid credentials to further their operations. Cyber espionage actors can also reuse their covert access to a victim's network for other purposes. For example, a malicious cyber actor could start using their access to a target network for disruptive and destructive purposes, if their intent shifts from espionage to disruption or destruction.

The boundary between state-sponsored and cybercriminal activity continues to be blurred. While state-sponsored cyber actors' intentions for the data they collect may differ from cybercriminals, the way in which they compromise systems and extract data is aligned in that they use similar tools, techniques and weaknesses in systems. State-sponsored cyber actors will continue to adapt their techniques, using both publicly available and bespoke tools to achieve their objectives.

Highlight 1: People's Republic of China cyber espionage targeting Australian and regional networks

In July 2024, ASD's ACSC released a cyber security advisory detailing the tradecraft of a People's Republic of China (PRC) state-sponsored group known as Advanced Persistent Threat (APT) 40. Industry also tracks this group as Kryptonite Panda, Gingham Typhoon, Leviathan and Bronze Mohawk. ASD's ACSC and international partners assess APT40 receives its tasking from the PRC's Ministry of State Security (MSS) – the agency responsible for foreign intelligence collection for the PRC.

APT40 regularly conducts malicious activities against Australian and regional networks that possess information of value to the PRC. These activities represent a security threat to many government and critical infrastructure networks. Australia and several international partners acted decisively to detail the tradecraft of APT40 to assist network defenders to detect and prevent their malicious activities.

APT40 is known for its rapid exploitation of security vulnerabilities, often within hours or days of the publication of proofs of concept. This shows its preferred initial access technique, which favours exploiting public-facing applications over other traditional methods like phishing. This highlights the defensive value of implementing relatively simple mitigation strategies, which continue to be effective at preventing actors like APT40.

ASD's ACSC and international partners have also observed APT40, alongside other actors, using botnets made up of compromised Small Office Home Office (SOHO) devices. The use of compromised devices allows APT40 to blend malicious traffic with the legitimate traffic of the device owner, complicating the detection and prevention efforts of network defenders.

Once initial access has been achieved, incident investigations have shown APT40 obtains access to legitimate user credentials to conduct further actions on the victim network, rather than making use of malware. This can further complicate the efforts of network defenders to detect and defend against the malicious activity.

APT40's approach observed over time is an example of state-based actors refining their tradecraft to continually evade detection and prevention efforts by network defenders.

APT40 Advisory: PRC MSS tradecraft in action is available at cyber.gov.au.

Cybercriminals

Cybercrime continues to challenge Australia's economic and social prosperity. Cybercrime is persistent and damaging across all facets of Australia's economy as financially motivated cybercriminals are willing to exploit any available opportunity for profit. ASD focuses on countering top-tier financially motivated cybercriminals and their enablers – we continue to see this threat emanating from the Eastern European region and Russian speaking cyber gangs. Cybercriminals continue to target Australia due to our widespread adoption of digital infrastructure, perceived population wealth and varied levels of cyber maturity.

Cybercriminals target Australian individuals and organisations for financial gain, attempting to conduct fraud or extortion through ransomware attacks or data theft. Cybercriminals are also likely to conduct multiple layers of extortion, where they not only encrypt a victim's network but also steal the data prior to encryption and threaten to release the data if their demands are not met. Cybercriminals have attempted to extort the primary network owner as well as the individuals or entities that are referred to in the data stolen.

In FY2024–25, ASD's ACSC received over 84,700 cybercrime reports through ReportCyber; however, ASD's ACSC assesses that the vast majority of cybercrime continues to go unreported.

The average self-reported cost overall was $36,633 – with identity fraud, online shopping fraud, and online banking fraud the most frequently reported cybercrime types. Identity fraud continues to be the most common cybercrime type reported by Australians. Identity fraud involves someone using another individual's personal information without consent, often to obtain a financial benefit.

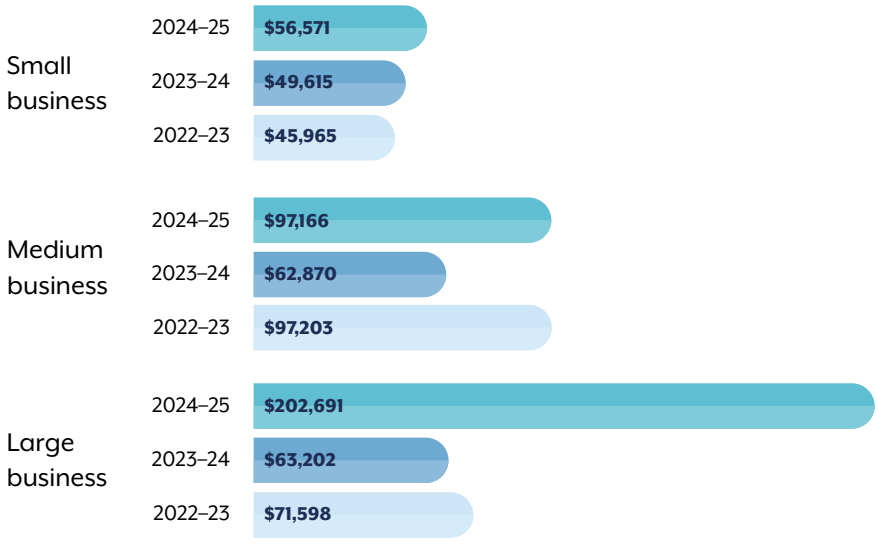


Figure 3: The average self-reported cost of cybercrime to businesses

Note: In FY2024–25, the average self-reported financial cost of cybercrime to large business increased by 219%. A portion of this increase may be driven by the 138% increase in total financial losses from BEC for large business. However, the increase in financial losses for large business may also be attributed to low reporting numbers, making the average cost susceptible to outliers. There was a 22% decrease in cybercrime reports made by large businesses compared to the previous financial year. Large businesses continue to have the lowest number of cybercrime reports (accounting for just over 12% of reports from all businesses) when compared to reports by small and medium businesses.

The Australian Institute of Criminology's (AIC) 2024 Australian Cybercrime Survey found that small-to-medium enterprise (SME) owners experienced significantly higher rates of all types of cybercrime in both 2023 and 2024. When they fell victim, SME owners were more likely to have lost money or spent money on consequences and, when they did, they lost larger amounts of money than other victims. In 2024, 22% of respondents who were SME owners said their business was impacted by cybercrime.

Criminal services continue to enable the cybercrime threat to Australia

Cybercrime-as-a-service allows cybercriminals to specialise in certain aspects of the ecosystem, making profit through the provision of services that support cybercriminal activities. The professionalisation of the cybercrime ecosystem continues to enable cybercriminals to conduct malicious activity at scale, making malware, tools and infrastructure more accessible to support their activities.

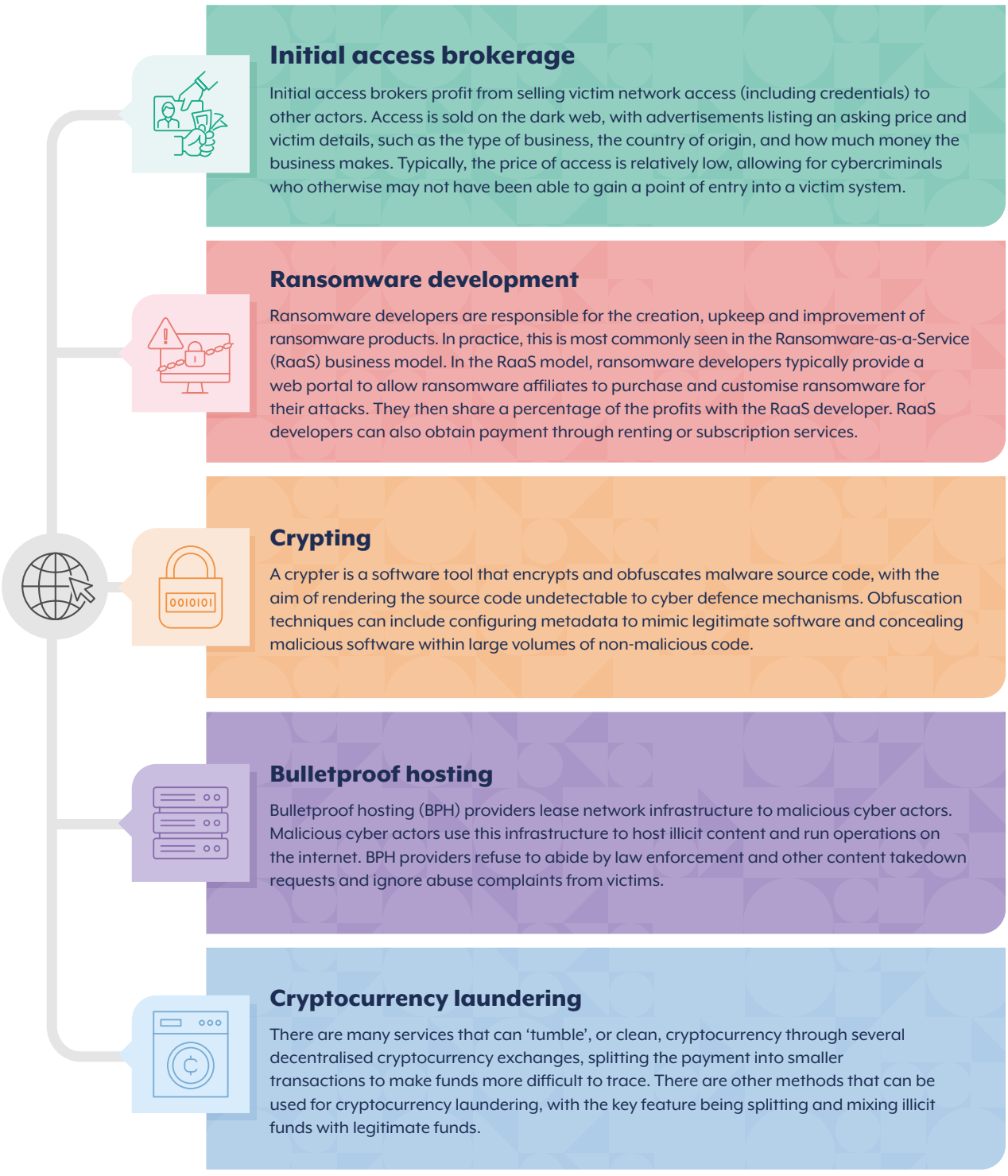


Figure 4: Examples of enabling services in the cyber extortion ecosystem

Ransomware continues to be lucrative for cybercriminals

Ransomware continues to be the most disruptive cybercrime threat in FY2024–25. In FY2024–25, ASD's ACSC responded to 138 ransomware incidents, 39% of which were the result of ASD's ACSC contacting the entity to warn of a possible cyber security incident.

Ransomware provides cybercriminals with lucrative opportunities to extort substantial ransoms from vulnerable Australian organisations. Ransomware is effective, high-impact malware that can cripple an organisation's ability to function. Ransomware causes serious operational, financial, and reputational consequences for victims while, in some cases, also threatening the security of the broader community. In April 2025, a large UK retailer was victim to a ransomware attack, costing the company an estimated £300 million ($618 million), which demonstrates the extreme costs that ransomware can have on victims.

On 30 May 2025 the Australian Government introduced a mandatory ransomware reporting regime for businesses with annual turnovers of $3 million or more and for entities responsible for CI. This regime aims to enhance the Government's visibility of ransomware and cyber extortion threats, enable tailored advice to industry, inform policy and legislation, and improve operational responses to disrupt ransomware activity across Australia.

Highlight 2: BianLian and Evil Corp sanctions

In November 2024, ASD's ACSC, in collaboration with US partners – the FBI and the Cybersecurity and Infrastructure Security Agency (CISA) – released an updated joint advisory on the BianLian ransomware group.

BianLian is a ransomware developer, deployer and data extortion cybercriminal group, likely based in Russia, with multiple Russia-based affiliates. The group have targeted Australian critical infrastructure sectors in addition to professional services and property development. They have also affected organisations in multiple US critical infrastructure sectors since June 2022.

Since January 2024, BianLian has used an exfiltration-based extortion model to demand payment from victim entities by threatening to post stolen data on the dark web. The malicious cyber actors have been observed using readily available tools and techniques to gain initial access, harvest credentials and exfiltrate data.

The advisory, *#StopRansomware: BianLian Ransomware Group*, is available at cyber.gov.au.

In further response to continued ransomware cyber threats, in October 2024, the Australian Government announced the imposition of financial sanctions and travel bans on 3 Russian nationals associated with the cybercrime group Evil Corp.

Maksim Viktorovich Yakubets, Igor Olegovich Turashev and Aleksandr Viktorovich Ryzhenkov were all subject to the imposed cyber sanctions due to their senior roles in Evil Corp. The group targeted and disrupted multiple sectors, including national infrastructure, government and the health sector, which also involves critical health systems.

Bulletproof hosting

BPH providers lease network infrastructure to malicious cyber actors. Malicious cyber actors use this infrastructure to host illicit content and run operations on the internet.

BPH providers are often advertised in underground forums as secure and resilient cyber infrastructure that can be used to store data associated with illicit cyber activities. Importantly, BPH providers knowingly participate in the cybercrime ecosystem and refuse to abide by law enforcement and other content takedown requests, and they also ignore abuse complaints from victims.

Criminals have used BPH providers to enable major cyber security incidents affecting Australian organisations and their customers. Consequences of these incidents have included disruptive ransomware attacks, data extortion and theft of sensitive data.

Countering the threat of illicit infrastructure providers

ASD's ACSC is working with partners across whole of government and the private sector to understand and respond to the threat posed by offshore illicit infrastructure providers to Australia, including BPH providers. Partners include domestic and international law enforcement, Cybersecurity Emergency Response Team (CERT) and intelligence partners, commercial threat intelligence vendors, and critical infrastructure and systems of national significance (CISONS).

With these partners, ASD's ACSC is working to prevent and counter the threat by:

- releasing indicators of compromise (IOCs) through ASD's ACSC's Cyber Threat Intelligence Sharing (CTIS) platform
- developing and releasing advisories on threats via ASD's ACSC's Partnership Portal
- uplifting the cyber hygiene of critical systems across Australia through targeted engagements
- joining with international partners to impose costs through mechanisms like cyber sanctions and server seizures
- Using ASD's unique cyber authorities to conduct offensive cyber operations to disrupt and destroy malicious infrastructure.

Highlight 3: Malicious website warning page

As part of its ongoing mission to protect Australians online, ASD's ACSC is proactively leveraging trusted strategic industry partnerships. By using Cloudflare's established API-based abuse reporting, it has been able to programmatically report malicious websites for prompt review and action.

This prompt reporting by ACSC helps Cloudflare verify and then display a phishing warning page that warns Australians of the potential dangerous activity. The warning page requires the user to physically click through to ignore the warning and this critical intervention serves as an immediate, frontline defence for Australians.

This has protected not only ASD's ACSC partners, but also all Australians interacting with the infrastructure from personal computers and portable devices.

Highlight 4: Further sanctions in response to cyber attacks against Australians

On 12 February 2025, the Australian Government imposed targeted sanctions, under the Autonomous Sanctions Regulations 2011, on a cyber infrastructure entity – ZServers – and 5 of its Russian employees. The individuals are ZServers' owner, Aleksandr Bolshakov, and employees Aleksandr Mishin, Ilya Sidorov, Dmitriy Bolshakov and Igor Odintsov. The sanctions were in response to ZServers' role in providing BPH services to host and disseminate data stolen from compromises of Australian and other organisations in 2022.

Australia's cyber sanctions are strengthened by tri-lateral sanctions imposed by the US and UK against these malicious cyber actors, demonstrating our collective resolve to combat cybercrime. These sanctions follow Australia's first cyber sanctions issued against Aleksandr Gennadievich Ermakov in January 2024, for his role in the Medibank Private data breach.

These latest sanctions make it a criminal offence to provide assets to ZServers or the 5 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. Cyber sanctions impose cost and consequence on cybercriminals' ability to operate.

Malicious cyber actors continue to target Australian governments, critical infrastructure, businesses and individuals. This threat will continue to be met by the collaborative work of the AFP, ASD's ACSC, the Department of Foreign Affairs and Trade, 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.

Information stealers simplify data theft for cybercriminals

Information stealer malware, also known as info stealers, is a type of malicious software designed to infect a device, collect as much valuable data as possible, and deliver it directly to cybercriminals.

Info stealers are commonly distributed through SMS or email phishing, online advertisements containing malicious links and downloads containing hidden malicious code. The malware is designed to extract data such as usernames and passwords, credit card details, cryptocurrency wallets, local files and browser data including cookies, user history and autofill details.

Malware-as-a-Service (MaaS) providers offer info stealers to entry-level cybercriminals on cybercriminal marketplaces, making info stealers an attractive method for cybercriminals with limited technical proficiency. These cost-effective subscription services allow cybercriminals to easily distribute malware and collect stolen data, which they can leverage and sell.

Cybercriminals may seek to purchase and use stolen user credentials associated with corporate accounts to gain initial access to the devices of the victim's employer, their clients and other enterprise systems. Subsequent impacts to these organisations can include ransomware, extortion, BEC and theft of intellectual property.

Cybercriminals may purchase and use an individual's stolen data to access personal email and social media or financial accounts, resulting in financial losses, loss of privacy and increased risk of identity theft.

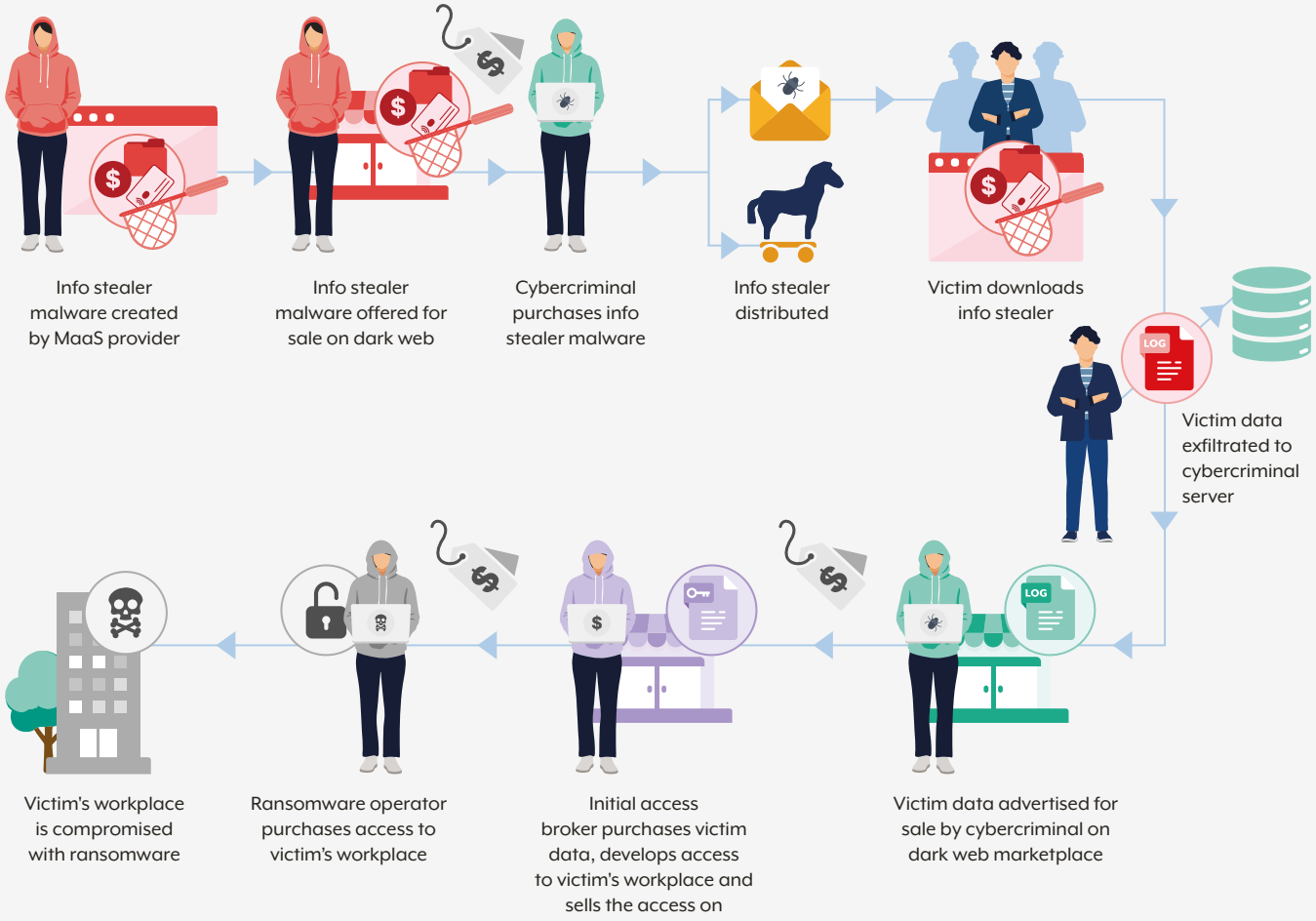


Figure 5: Example of an info stealer ecosystem and possible impact on an organisation

Case study 1: Info stealer incident

In mid–2024, ASD's ACSC became aware that credentials potentially belonging to a utility company were compromised, probably through information stealer malware. ASD's ACSC notified the company's security operations centre, who promptly initiated an investigation.

The utility company's investigation revealed that an employee's personal device had been compromised with an info stealer. The credentials were probably moved from a corporate asset when the employee logged into a personal Google account on their work device and synchronised work credentials to their Google account. When the employee's personal device was compromised, the information stealer was able to extract the work credentials from the browser on their personal device. The company noted this has become an increasingly common issue.

The company guided the employee on how to remove the malware from their personal device and perform scans to confirm removal. An initial sweep of the corporate device was also performed. There was no evidence that credentials were exploited; had an attempt to exploit the credentials occurred, the risk to the company was partly mitigated through multi-factor authentication (MFA) and internal credential rotation.

Organisations which permit employees to access personal accounts on corporate devices need to be aware of the risks of information stealers and protect themselves from this threat.

For more information, see: *The silent heist: cybercriminals use information stealer malware to compromise corporate networks,* which is available at cyber.gov.au.

Responding to the threat of info stealers

ASD is working with partners across whole of government and the private sector to understand and disrupt the threat posed to Australia by information stealer malware. Partners include domestic and international law enforcement; CERT and intelligence partners; commercial threat intelligence vendors; technology vendors; and CI operators.

With these partners, ASD is working to prevent and counter this threat by:

- releasing IOCs through ASD's CTIS platform, including notifying affected organisations of compromise to enable remediation where available
- expanding of ASD's credential exposure notification process through the Cyber Hygiene Improvement Programs (CHIPs) with 9,587 credential exposure events proactively sent to approximately 220 organisations during the period from 19 November 2024 to 30 June 2025
- developing and releasing advisories on threats via ASD's ACSC's Partnership Portal
- conducting awareness raising campaigns with practical advice for the everyday Australian to protect themselves
- uplifting cyber hygiene of critical systems across Australia through targeted engagements.

Under Operation Aquila, ASD and the AFP pursue cybercriminals who employ information stealer capabilities against Australians and our partners via our offensive cyber capabilities. Our skilled offensive cyber operators use an array of specialist tools and techniques to find weaknesses in the systems and tradecraft used by those who seek to unlawfully gain access to Australian networks. The use of offensive cyber is applied on a proportionate and necessary basis to prevent further incidents of cybercrime and introduce cost and consequence to those who conduct these activities.

Operation Aquila is the Joint Standing Operation between the AFP and ASD that identifies and disrupts the highest priority cybercriminals targeting Australia.

Explainer 1: Office of Australian Information Commissioner (OAIC) Notifiable Data Breaches scheme statistics

The OAIC publishes Notifiable Data Breach statistics every 6 months. The most recent report noted the OAIC received 595 data breach notifications between July and December 2024, an increase of 15% compared to the previous 6 months.

2024 marked the highest number of notifications in a year since the OAIC's *Notifiable Data Breaches scheme* commenced in 2018. This reflects the continuing information security challenges faced by Australian organisations, but also the growing maturity of their data breach detection and reporting practices. The reporting period from July to December 2024 saw a significant increase in data breaches caused by social engineering and impersonation – the manipulation of people into carrying out specific actions or divulging information. For more information on the threat of social engineering and mitigation advice see page 33 of the report or visit cyber.gov.au.

Cybercriminal use of generative artificial intelligence

Generative Artificial Intelligence (GenAI) has the potential to generate significant benefit for the Australian economy and society. It also creates an avenue for cybercriminals to streamline and scale their activities. GenAI models are a type of AI that can create new content, including text, code, images and videos, based on previous learning and user prompts.

Cybercriminals use GenAI to automate the analysis of extensive datasets, such as identifying valuable credentials or extortion material in stolen data.

Cybercriminals also use GenAI to create high-quality videos, fake voices, websites, know-your-customer records and spearphishing emails to more convincingly present themselves to victims as legitimate actors with relatively minimal effort.

Global law enforcement disruption efforts

Cybercrime is borderless in nature and requires significant international collaboration to be countered effectively. During FY2024–25, global law enforcement disruption efforts have successfully prevented harm against Australian individuals and organisations, including through the disruption of a scam centre suspected of stealing money from Australians.

Highlight 5: Operation Firestorm

In April 2025, AFP's Operation Firestorm collected intelligence that a scam centre in Bangkok, Thailand, was being established to target Australians with investment bond scams. Information indicated that during a previous scam operation between January and February 2025, the syndicate successfully deceived Australian victims into investing $28 million.

In June 2025, under Operation Firestorm-Apiarist, AFP investigators supported the Royal Thai Police with the disruption of the identified scam centre resulting in the arrest of 13 persons, including 5 Australian nationals.

As part of the pitch to build trust and fleece their victims, syndicate members used a well-orchestrated and detailed script involving high-pressure tactics and forged documentation to pretend to represent an international financial firm selling high-yield fixed-income bonds.

During early law enforcement disruption, 12 Australians were identified as victims of the scam, having transferred funds to fake accounts. Items found at the property suggested the scammers amassed more than $1.9 million in suspected stolen funds from Australians in just 2 months of its operation.

The AFP-led Joint Policing Cybercrime Coordination Centre (JPC3) Operation Firestorm collaborates with foreign law enforcement agencies to coordinate the disruption of cyber-enabled fraud that targets Australians. Operation Firestorm focuses on delivering accurate, real-time intelligence relating to scam centres operated by organised crime groups, with the objective of disrupting, arresting and prosecuting individuals and groups involved in offshore cyber-enabled fraud.

What **malicious cyber actors** are targeting

- Both individuals and businesses are commonly targeted by malicious cyber actors for financial gain. This can be through scams or through the on-selling of personally identifiable information (PII) or usernames and passwords online.
- State-sponsored cyber actors continue to target networks across government and industry to support political, economic and military objectives.
- CI may be targeted by malicious cyber actors to conduct espionage, degrade confidence in systems, interrupt service availability, or pre-position for disruptive or destructive effects.

Everyone can be a target

Any individual or organisation using digital technology can be the target of a malicious cyber actor. While many cyber incidents are opportunistic in nature, malicious cyber actors routinely target both entities and individuals in specific sectors due to the information they hold or the services they provide.

Those aged 25–34 and 35–44 continue to be the age groups reporting most often to ReportCyber (accounting for 42% of all reporters). FY2024–25 also saw an increase in reporting from victims aged 55–64 and 65+ (accounting for 24% of all reporters).

Highlight 6: BADBAZAAR and MOONSHINE spyware

On 9 April 2025, ASD's ACSC joined international partners to publish an advisory raising awareness of the growing threat that malicious cyber actors pose to individuals who are connected to topics, including Taiwan, Tibet, Xinjiang Uyghur Autonomous Region, democracy movements and the Falun Gong. The advisory detailed 2 case studies involving mobile-device spyware known as BADBAZAAR and MOONSHINE.

The advisory, *BADBAZAAR and MOONSHINE: Spyware targeting Uyghur, Taiwanese and Tibetan groups and civil society actors* is available at cyber.gov.au.

Compared to FY2023–24, financial and insurance services rose to be the most frequently reporting non-government sector. Some of this rise is attributable to DDoS activity targeting the financial sector. Education and training dropped out of the top 5 reporting sectors, while reporting from the electricity, gas, water and wastewater services sector was down from 5% to 2% of all incidents.

Within the government sector, Federal Government reporting was down from 37% to 32%, while state and local government reporting was up from 12% to 14% of all incidents.

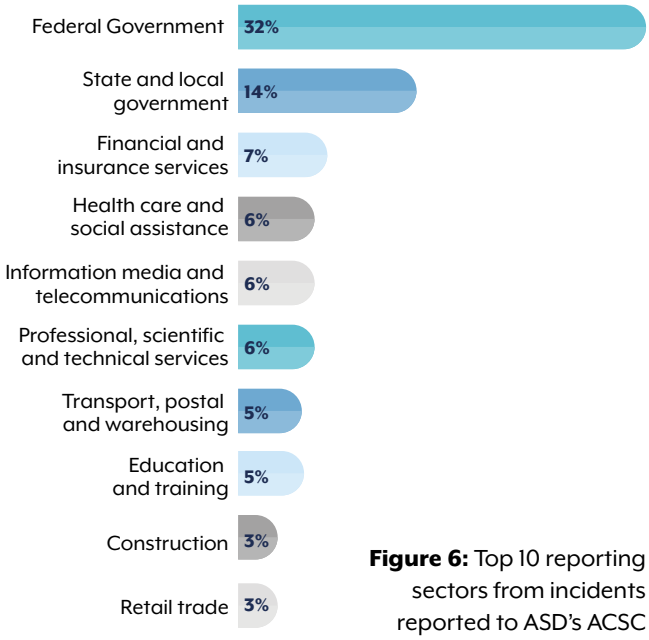
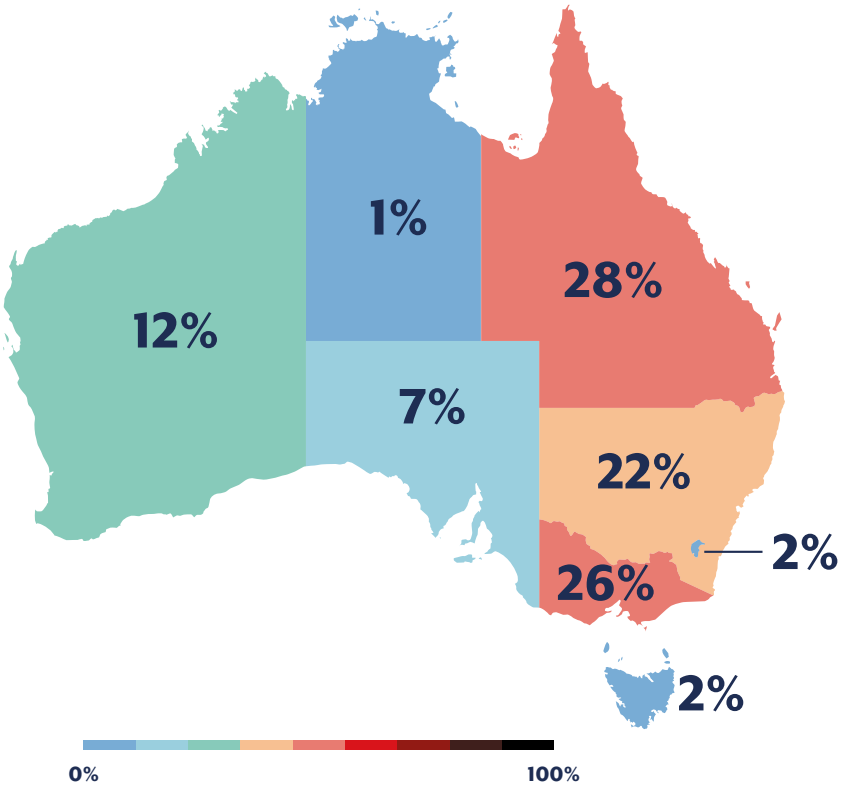


Figure 6: Top 10 reporting sectors from incidents reported to ASD's ACSC

Cybercrime reports by state and territory



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

The Australian Capital Territory reported the highest average self-reported financial losses – around $37,700 per cybercrime report – followed by those in New South Wales, with around $33,000. Northern Territory also closely followed with around $32,000 per cybercrime report where a financial loss occurred.

Figure 7: Breakdown of cybercrime reports by jurisdiction for FY2024–25

Critical infrastructure

CI is, and will continue to be, an attractive target for state-sponsored cyber actors, cybercriminals and hacktivists, largely due to the sensitive data it holds and its role in providing services that support Australia's national resilience, sovereignty and prosperity.

State-sponsored cyber actors routinely target Australia's CI networks, possibly to conduct espionage or to pre-position for disruptive and destructive cyber effects in the event of crisis or conflict. In crisis or conflict, access to a CI network can provide a malicious cyber actor with control over Australia's CI systems, which could lead to a degradation in the confidence of systems, major disruptions to availability, or even destructive effects.

Cybercriminals continue to opportunistically target CI operators. The sensitivity of the data stored by these entities, and the importance of their services, makes them attractive for cybercriminals seeking to extort victims.

CI often relies on complex information technology (IT) and operational technology (OT) networks, with complex supply chains. While these networks allow CI providers to deliver services to the Australian people, they also present an ever-growing attack surface, which includes both the provider themselves and those within their supply chain.

CI made up **13%** of all incidents, **up 2%** from last year

The 3 most common **activity types** leading to critical infrastructure-related incidents were:

- Scanning or Reconnaissance **(41%)**
- DoS/DDoS **(31%)**
- Phishing **(20%)**

Top 3 **ANZSIC Divisions for CI incidents:**

- Financial and insurance services **(32%)**
- Transport, postal and warehousing **(26%)**
- Information media and telecommunications **(16%)**

Highlight 7: Russian GRU targeting Western logistics entities and technology companies

In May 2025, ASD's ACSC joined international partners in highlighting a Russian state-sponsored cyber campaign targeting Western logistics entities and technology companies. This includes those involved in the coordination, transport and delivery of foreign assistance to Ukraine.

For over 2 years, the Russian General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (85th GTsSS), military unit 26165 – commonly known in the cyber security community as APT28, Fancy Bear, Forest Blizzard, BlueDelta, and a variety of other identifiers – has conducted this campaign using a mix of known TTPs, including reconstituted password spraying capabilities, spearphishing, and modification of Microsoft Exchange mailbox permissions.

In late February 2022, multiple Russian state-sponsored cyber actors increased the variety of cyber operations for purposes of espionage, destruction, and influence – with unit 26165 predominately involved in espionage. As Russian military forces failed to meet their military objectives and Western countries provided aid to support Ukraine's territorial defence, unit 26165 expanded its targeting of logistics entities and technology companies involved in the delivery of aid. These actors have also targeted internet-connected cameras at Ukrainian border crossings to monitor and track aid shipments.

The advisory, *Russian GRU targeting Western logistics entities and technology companies* is available at cyber.gov.au.

IN FOCUS: The threat to telecommunications providers

Malicious cyber actors continue to target the telecommunications sector globally for espionage purposes. Telecommunications networks are attractive targets because of the valuable data they store and communicate. Access to these networks can also enable follow-on targeting of telecommunications customers. Sustained disruption of telecommunications services would probably cause follow-on disruptive effects to other CI entities who rely on telecommunications for internet and phone services.

On 4 December 2024, ASD's ACSC joined international partners to publish an advisory warning that PRC-affiliated malicious cyber actors had compromised the networks of major global telecommunications providers as part of a broad and significant cyber espionage campaign.

The advisory provides network engineers and defenders of communications infrastructure with best practices to strengthen their visibility and harden their network devices against successful exploitation carried out by PRC-affiliated and other malicious cyber actors.

The advisory, *Enhanced visibility and hardening guidance for communications infrastructure*, can be found at cyber.gov.au.

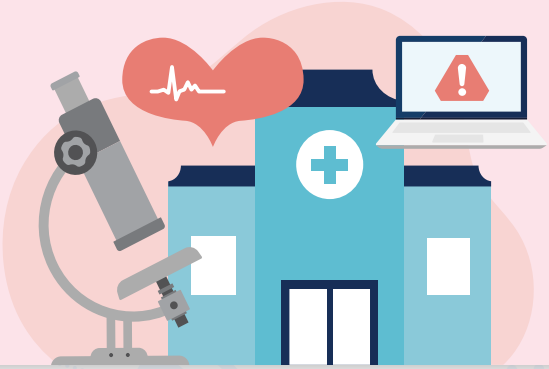
IN FOCUS: The threat to the healthcare sector

Disruption of Australian healthcare networks can endanger patients, making the healthcare sector vulnerable to extortion by cybercriminals. Healthcare data is also valuable on dark web forums as it directly enables other criminal activities, like fraud and identity theft.

The frequency of cybercrime incidents against the healthcare sector in Australia is increasing. Compared to FY2023–24, the number of ransomware incidents against the healthcare sector doubled in FY2024–25, endangering patient safety and destabilising health systems. Malicious cyber actors were successful in 95% of all health care and social assistance sector incidents that ASD's ACSC responded to in FY2024–25, in comparison to nearly 52% of incidents across all sectors.

In July 2024, an e-prescription service notified customers of a cyber security incident. With the assistance of the AFP under the joint arrangement Operation Aquila, the incident was investigated with support from ASD's ACSC.

In a suspected ransomware attack, malicious cyber actors exfiltrated approximately 6.5TB of data from the e-prescription services database server that had data stored from March 2019 to November 2023. This data included the personal and health information of approximately 12.9 million Australian customers who used the e-prescription service during this time.



Common techniques used by malicious cyber actors

- ASD's ACSC has observed a range of common techniques that malicious cyber actors use to exploit vulnerabilities in technology and systems, which we map against the MITRE ATT&CK framework.
- Identifying and understanding exposure to these vulnerabilities is a critical first step towards reducing the risk of successful compromise by these actors.
- *Chapter 2: Resilience* outlines steps that can make it harder for malicious cyber actors to successfully exploit these vulnerabilities.

Analysing incidents using the MITRE ATT&CK framework

The MITRE ATT&CK framework is an open-source knowledge base of adversary tactics and techniques, derived from real adversary observations, which provide a common language for describing, understanding and analysing cyber threats.

Adversary behaviours are organised into a matrix – tactics, the 'goal' of the adversary; and techniques, the 'approach' of the adversary. ATT&CK empowers organisations to mature their cyber security posture through detection and mitigation strategies based on real-world observed adversary behaviours.

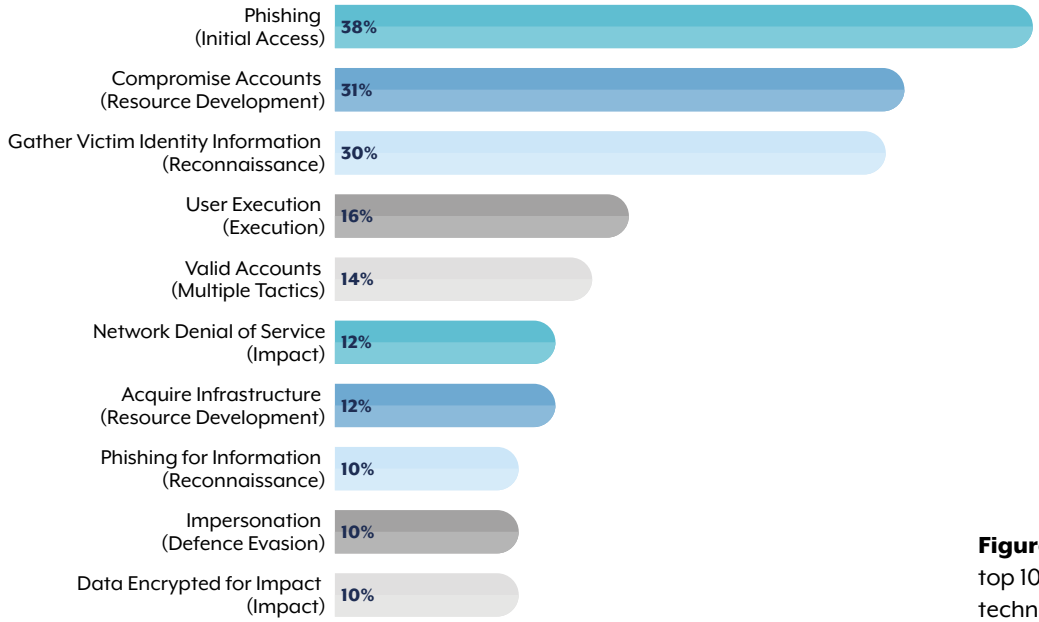


Figure 8: Prevalence of top 10 MITRE ATT&CK techniques in FY2024–25

Note: The occurrence of MITRE ATT&CK techniques does not total 100% as multiple techniques can be identified in each incident. Technique prevalence will also likely skew towards techniques that occur across multiple tactics, and to pre-compromise techniques, as not all incidents are successful.

Differences in reported techniques between government and industry reporting

Government Incidents	Industry Incidents
Phishing (52%)	Phishing (25%)
Compromise Accounts (39%)	Compromise Accounts (24%)
Gather Victim Identity Information (38%)	Gather Victim Identity Information (23%)
User Execution (22%)	Valid Accounts (23%)
Acquire Infrastructure (16%)	Data Encrypted for Impact (18%)
Phishing for Information (15%)	Exploit Public-Facing Application (10%)
Network Denial of Service (15%)	User Execution (10%)
Impersonation (11%)	Network Denial of Service (10%)
Compromise Infrastructure (10%)	Financial Theft (9%)
Stage Capabilities (9%)	Brute Force (9%)

Figure 9: Top 10 MITRE ATT&CK techniques in government and industry reporting

Over FY2024–25, Phishing, Compromise Accounts, and Gather Victim Identity Information were the top 3 observed techniques across government and non-government incident reports.

Government reporting predominately featured techniques early in the cyber attack chain. Conversely, 18% of industry reporting involved data encrypted for impact compared to <1% in government reporting. This technique is often observed in ransomware incidents in which a cyber threat actor encrypts data to demand a ransom. Similarly, Exploit Public-Facing Application (10%) and Financial Theft (9%) were much higher than in government entities (2% and 1% respectively).

This may reflect a number of different factors, including different reporting cultures and requirements, or awareness of where to report in the event of a cyber incident.

Initial access techniques in data encryption incidents

In FY2024–25, ASD's ACSC observed that, in incidents where data was encrypted for impact, the most common means of gaining initial access was through using already compromised credentials (Valid Accounts) and accessing networks via legitimate external-facing services (External Remote Services).

Social engineering

Social engineering is a longstanding threat that is becoming easier for malicious cyber actors to use at scale, thanks in part to AI technologies.

Phishing – a type of social engineering – was recorded as an initial access technique in 38% of the incidents reported to ASD's ACSC in FY2024–25.

Social engineering techniques are used by malicious cyber actors to direct individuals or staff into performing specific actions such as opening an attachment, visiting a website, revealing credentials, disclosing sensitive information, or transferring funds. Social engineering techniques can be highly convincing.

If you suspect a social engineering attempt, do not engage – hang up. Do not delete or forward the communication. Report it immediately to your organisation's cyber security or IT support team for advice. Preserving the communication is important for investigation and threat response.

Denial of Service

DoS attacks are cyber attacks designed to disrupt or degrade online services such as websites, email and Domain Name System (DNS) services, in order to deny access to legitimate users. A DDoS attack is a type of DoS attack using multiple computers or other internet-connected devices to direct network traffic at online services, from multiple directions and on a much larger scale.

DDoS is becoming increasingly available to a range of actors, regardless of technical proficiency. Growth in areas such as AI, as well as a growing botnet attack surface, is lowering the bar for less capable adversaries to engage in DDoS attacks. AI empowers a DDoS attack through autonomously running algorithms that manage complex botnets. Additionally, by using AI to manage botnets, malicious cyber actors can rapidly adjust their code to evade detection.

The rise of DDoS attacks against Australian organisations has the potential to cause significant disruptions across the Australian economy. ASD's ACSC responded to more than 200 incidents involving DoS or DDoS attacks, up more than 280% from last year. DoS and DDoS were present almost twice as often (31%) in incidents against CI entities when compared with all incidents ASD's ACSC responded to (16%).

Additionally, industry reporting indicates that June 2025 may have had the most DDoS incidents on record. This increase follows an obvious upwards trend in the number of reported DDoS attacks over the last 5 years, with FY2021–22 having had more than 20 DDoS attacks, while FY2022–23 had more than 50.

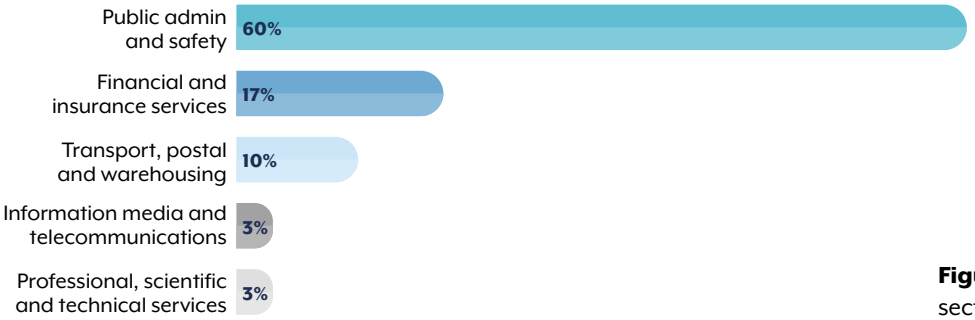


Figure 10: Top 5 reporting sectors for DoS/DDoS incidents

In March 2025, ASD's ACSC, in cooperation with New Zealand's National Cyber Security Centre (NCSC-NZ), Akamai Technologies Ltd and Cloudflare Pty Ltd, published updated advice on preparing for and responding to DoS attacks. For more information visit *Preparing for and responding to denial-of-service attacks* on cyber.gov.au.

Vulnerabilities create opportunities

Malicious cyber actors often rely on common gaps in cyber defences to achieve their objectives. There are also emerging security challenges that will create more opportunities for malicious cyber actors to target Australia.

Stolen data

Malicious cyber actors often use stolen personal information to appear legitimate and improve the success rate of their phishing campaigns. They can also use stolen credentials to gain access to other networks or accounts that use the same or similar credentials. Many individuals and organisations are not aware of the full extent and criminal value of their sensitive information published online.

Vulnerable devices and software

Malicious cyber actors commonly exploit vulnerable devices and software. In FY2024–25, the number of publicly reported common vulnerabilities and exposures increased by 28%. Edge devices and legacy IT are notable examples of systems that are often difficult for network defenders to secure effectively.

IT supply chains

An organisation's supply chain can often be its weakest link. Malicious cyber actors may attempt to compromise an end consumer at multiple points in the supply chain, exploiting trusted relationships between the vendor and the customer to steal information or deliver malware or vulnerable products.

Gaps in event logging

Malicious cyber actors thrive when target organisations lack an established baseline or logging policy that support effective detection and response. Malicious cyber actors can exploit gaps in event logging to evade detection and even retain unauthorised access after a victim investigates the compromise.

Edge devices

ASD's ACSC often sees malicious cyber actors using vulnerabilities in edge devices to achieve their goals. Edge devices are critical network components, positioned at the network's periphery – often referred to as 'the edge'. These devices connect a private network, such as your home or work, with a public, untrusted network like the internet. The most common edge devices used include home and enterprise routers, firewalls and virtual private network (VPN) products.

Edge devices are attractive targets for malicious cyber actors because internet-facing vulnerabilities in edge devices are common, and they are often difficult for network owners to monitor or configure securely. These vulnerabilities provide malicious cyber actors with a greater chance of successfully compromising a network. By successfully exploiting such technologies, malicious cyber actors can gain an initial foothold on a network for follow-on activity. Malicious cyber actors can also use compromised edge devices as proxies, which can help hide their identity when targeting other networks.

In FY2024–25, ASD's ACSC observed more than 120 incidents associated with attacks on edge devices, of which 96% were successful.

In FY2024–25, ASD's ACSC released and co-sealed a series of publications focusing on improving the security and resilience of edge devices against cyber threats. These publications were supported by international partners including the US, Canada, New Zealand, UK and Japan. These publications are available at cyber.gov.au.

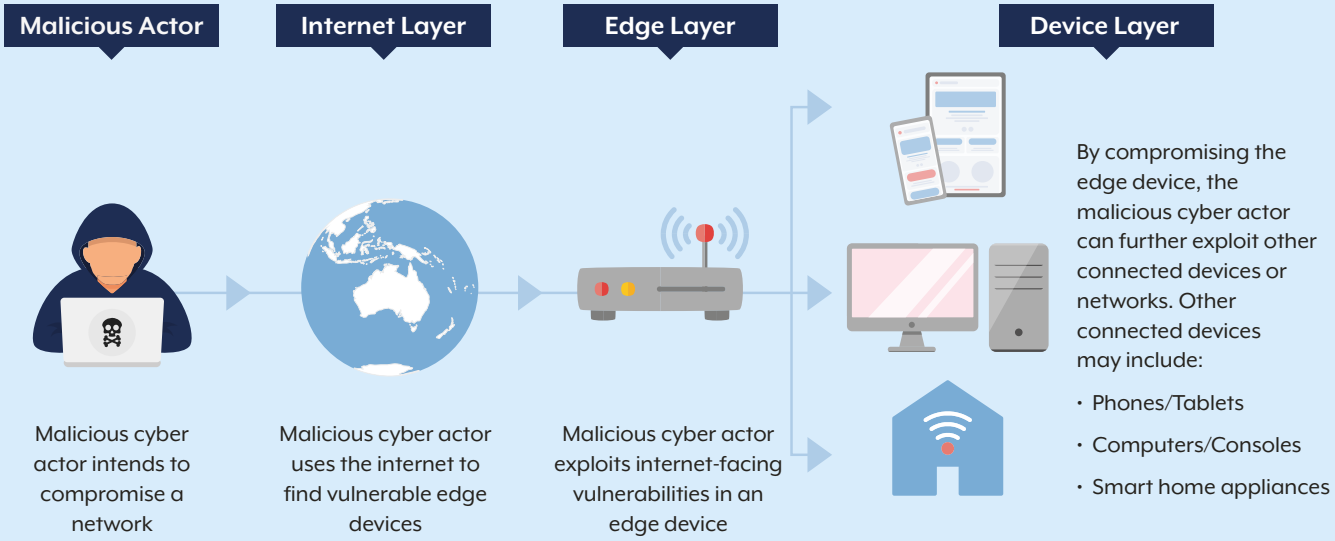


Figure 11: How network edge devices may be exploited for follow on activity

Highlight 8: PRC-linked cyber actors compromise routers and Internet of Things devices for botnet operations

In September 2024, ASD's ACSC joined international partners to publish an advisory that highlights the threat posed by PRC-linked cyber actors' botnet activity.

PRC-linked cyber actors had compromised thousands of internet-connected devices, including SOHO routers, firewalls, network-attached storage and Internet of Things (IoT) devices to create a network – or 'botnet' – positioned for malicious activity. The botnet consisted of over 260,000 devices, including devices in Australia. The cyber actors may use botnets like this as a proxy to conceal their identities while they deploy DDoS attacks or further target and compromise networks.

The advisory, *People's Republic of China-Linked Actors Compromise Routers and IoT Devices for Botnet Operations* can be found on cyber.gov.au.

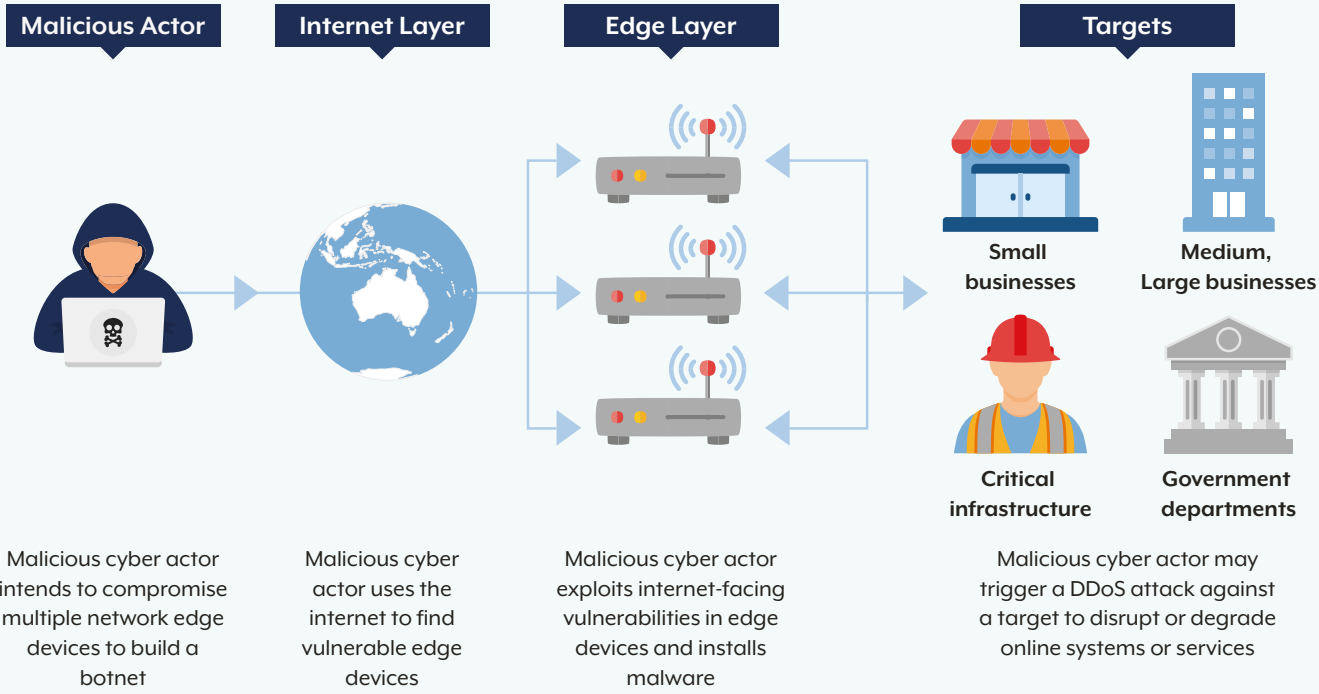


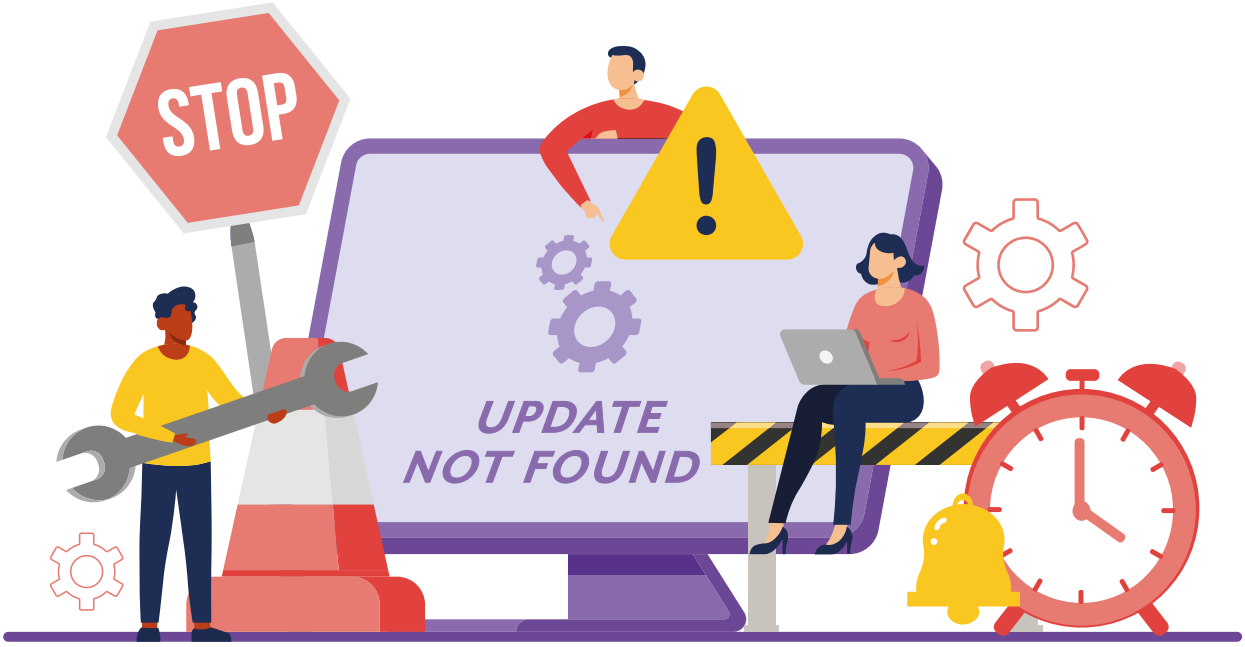
Figure 12: How network edge devices may be used as a botnet

Legacy IT

Legacy IT is hardware, software, services, protocols and/or systems that are considered end-of-life or are no longer supported by the vendor or developer.

Keeping legacy IT on a network increases the likelihood of a cyber security incident. It can also make any cyber security incident that does occur much more impactful. For example, malicious cyber actors can use legacy IT to gain an initial foothold on a network, or to gain access to more modern systems that organisations rely on.

There are also significant business risks associated with legacy IT. For example, legacy IT can increase the likelihood that an organisation will have systems taken offline, service delivery disrupted, data destroyed or leaked, and public confidence lost.



Chapter 2

Resilience

What **you can do**

- The basics are still our most effective first line of defence. All Australian small businesses and individuals should use strong MFA wherever possible, use strong and unique passwords or passphrases, keep software on devices updated, be alert for phishing messages and scams, and regularly back up important data.
- For businesses running a network, there are 4 big moves you can make to protect yourself: implement effective logging, replace legacy IT, effectively manage third-party risk and start preparing for post-quantum cryptography.
- For businesses that also manage OT, follow best-practice guidance for isolating vital OT and enabling systems, and have a plan for how to rebuild.
- Have a cyber security incident response plan and test it regularly to ensure a prioritised and effective response to an incident. It is vital that suspicious activity, cyber security incidents, and vulnerabilities are reported to ASD's ACSC at cyber.gov.au/report.

Resilience for all Australians

For small businesses and individuals, the basics have never been more important. Everyone can take steps to protect their most valuable asset – their information – and significantly reduce personal risks while engaging technology. The most effective cyber defences are also some of the easiest to use and fastest to setup. The top things Australians can do are:

- Use phishing-resistant MFA wherever possible, preferably passkeys
- If you use passwords or passphrases, make them strong and unique, and consider using a reputable password manager
- Regularly back up important files and device configuration settings
- Be alert for phishing messages and scams
- Keep software on devices updated, and only use a trusted device when accessing sensitive online accounts
  - For example, use your bank's app on your smartphone to perform internet banking
- Report cyber incidents to ASD's ACSC.

At cyber.gov.au, ASD's ACSC has published a range of simple how-to guides for all Australians, including children and seniors, that explain how individuals and families can improve their home cyber security.

The 4 key actions for organisations

You can't defend what you can't see
Implement effective event logging

Logging is crucial for detecting threats and keeping networks secure. Effective event logging can provide critical insights into a cyber security incident and reduce the overall cost of responding to them.

In August 2024, ASD's ACSC, in cooperation with international partners, published *Best practices for event logging and threat detection*.

In May 2025, ASD's ACSC also jointly published a suite of guidance to assist organisations implement Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) platforms.

These publications can be found on cyber.gov.au.

Old technology lets threats thrive
Manage legacy IT risks

Remediating a cyber security incident involving legacy IT, and managing its consequences, may involve high financial costs. It is always less costly to mitigate the risks of legacy IT before a major cyber security incident occurs.

The most effective strategy to eliminate the risks associated with legacy IT is to replace it with IT that is still receiving support – whether that support is internal or external. Where this is not feasible, or replacing legacy IT will take time, temporary measures should be adopted to mitigate some of the risk.

For more information on managing the risks of legacy IT, visit cyber.gov.au.

Shut the back door

Choose secure and verifiable technologies

The security of an organisation's supply chain for the digital products and services they operate is paramount as malicious actors may attempt to compromise an end consumer at multiple points in their supply chain.

The procurement of any digital product or service increases the attack surface of an organisation's information environment. It is critical to understand the threat environment and the possible supply chain attack vectors so organisations can identify and manage the risks through pre-purchase and post-purchase risk management.

In December 2024, ASD's ACSC published an updated version of its *Choosing Secure and Verifiable Technologies* and an accompanying executive guidance publication. Both publications were co-sealed with our international partners in the US, Canada, UK, New Zealand and the Republic of Korea, as part of the global campaign for secure-by-design.

Plan, educate, anticipate

Start preparing for post-quantum cryptography

A cryptographically relevant quantum computer (CRQC) is on the horizon, which means Australia must start preparing for post-quantum cryptography (PQC).

A CRQC is a quantum computer capable of breaking contemporary public key cryptography. The creation of a CRQC presents new cyber security risks as adversaries may use CRQC capabilities to compromise communications based on current public key cryptography technology.

PQC is the best way to protect our networks from the future quantum computing threat. PQC uses cryptographic algorithms that are different to the algorithms used in public key cryptography and are highly unlikely to be broken by a CRQC.

For more information, visit *Guidelines for Cryptography and Planning for Post-Quantum Cryptography* on cyber.gov.au.

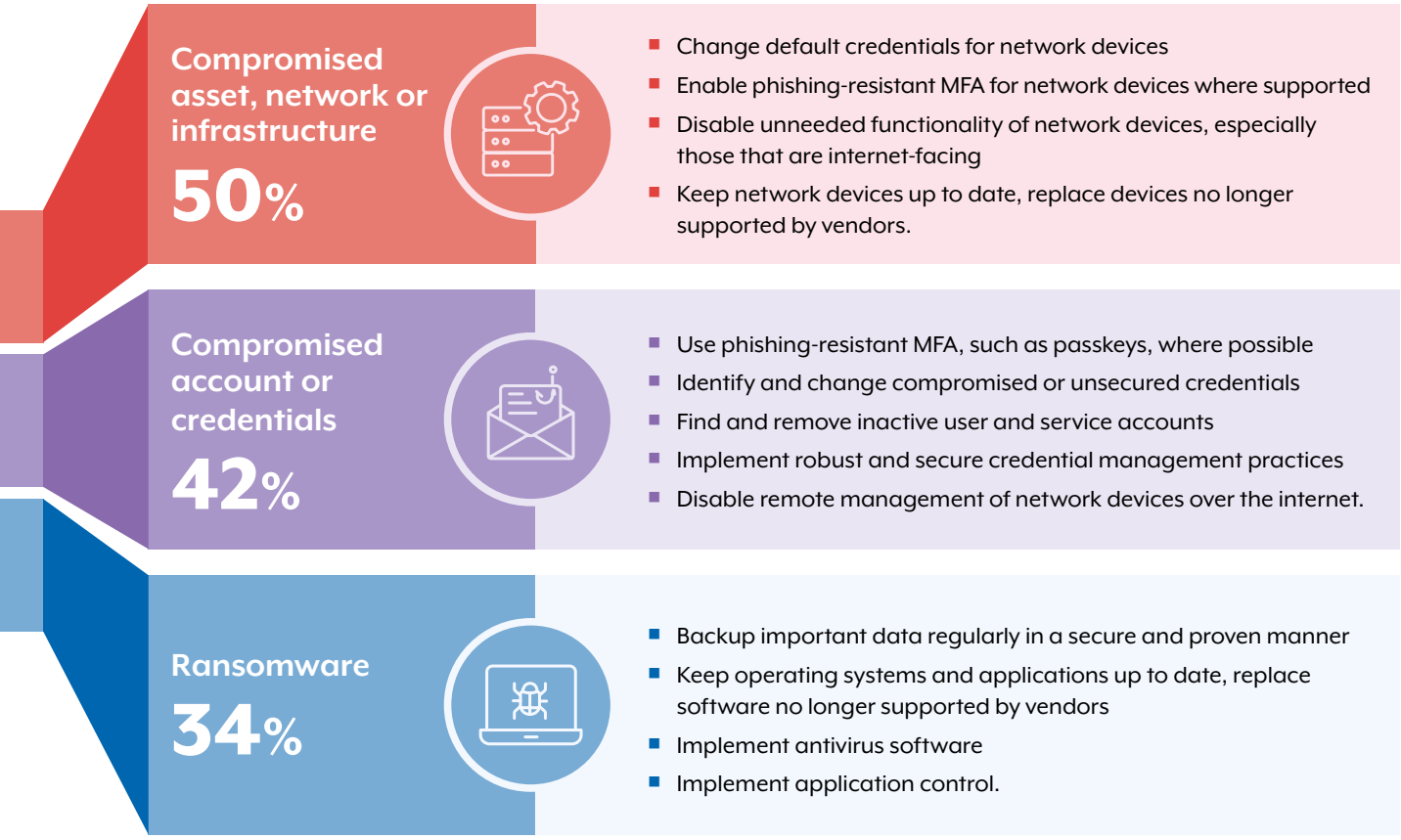


Figure 13: Top 3 reported incidents categorised C3 and above, with relevant mitigations

Note: Incidents can have multiple incident types ascribed to them and hence do not add up to 100%. Incidents categorised as C3 or above involved organisations such as federal and state governments, large organisations, academia, and supply chains.

Plan for the adoption of technologies with modern defensible architecture

In February 2025, ASD's ACSC published the *Foundations for modern defensible architecture* (the Foundations). Modern defensible architecture (MDA) aims to assist organisations to prepare and plan for the adoption of technologies based on:

1. zero trust principles of 'never trust, always verify', 'assume breach' and 'verify explicitly', implemented through zero trust architecture
2. secure-by-design practices to institute a security mindset within organisations when it comes to procuring or developing software products and services.

The Foundations provide a framework for secure design and architecture activities that will best prepare organisations to adapt to current and emerging cyber threats and challenges. Each foundation represents an organisational goal or capability that will promote a more efficient adoption of zero trust technologies.

The Foundations offer additional secure design and architecture advice as a structural framework upon which to implement ASD's ACSC's *Information Security Manual* (ISM) and ASD's ACSC's *Essential Eight Maturity Model*.

Further information on the Foundations can be found on cyber.gov.au.

Implement the Essential Eight

ASD's ACSC prioritised mitigation strategies – the *Strategies to Mitigate Cyber Security Incidents* – help organisations protect their enterprise IT networks against various cyber threats. The most effective of these mitigation strategies are the Essential Eight.

- patch applications
- patch operating systems
- multi-factor authentication
- restrict administrative privileges
- application control
- restrict Microsoft Office macros
- user application hardening
- regular backups.

Organisations are strongly encouraged to adopt the latest version of the *Essential Eight Maturity Model* to protect themselves against contemporary tradecraft used by malicious cyber actors.

Further information on the *Essential Eight Maturity Model* and its implementation is available in the *Essential Eight Maturity Model FAQ* publication on cyber.gov.au.

Apply the Information Security Manual

ASD's ACSC's ISM is a cyber security framework that an organisation can use to protect their systems and data from cyber threats. The ISM is intended for chief information security officers, chief information officers, cyber security professionals and IT managers.

The ISM is updated regularly; the latest version was released in June 2025. A map between the *Essential Eight Maturity Model* and the ISM is provided within the *Essential Eight Maturity Model and ISM Mapping* publication.

The ISM and guidance on how to implement the ISM can be found on cyber.gov.au.

Protect critical infrastructure networks with CI Fortify

To confront the threat of state-sponsored cyber actors targeting CI, ASD's ACSC released CI Fortify, the first in a new series of guidance, with 2 immediate priorities for CI operators:

- the ability to isolate vital OT and enabling systems from other networks and systems for 3 months
- the ability to completely rebuild vital OT and enabling systems.

CI Fortify reflects ASD's ACSC's proactive approach to defending Australia's most vital critical services. The guidance helps CI operators reduce attack surfaces and maintain critical service continuity, even during sustained cyber security incidents.

For more information, visit cyber.gov.au.

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, which is the Australian Government's technical authority on cyber security. 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 ASD's ACSC representative 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.

Cyber security incidents

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.

If ASD's ACSC assesses that the incident requires a more tailored approach, 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 information provided by you without your express consent. We are legally bound to only use your information for cyber security purposes to assist you and protect the Australian community. Your confidentiality is further protected under ASD's ACSC's 'limited use' obligation.

Limited use

To bolster a freer flow of information sharing between industry and ASD's ACSC, on 25 November 2024, the Australian Government passed the *Intelligence Services and Other Legislation Amendment (Cyber Security) Act 2024*. The amendment legislates a 'limited use' obligation for ASD's ACSC. This means any information that an Australian organisation voluntarily provides to ASD's ACSC about a cyber security incident or potential cyber security incident (including vulnerability information) cannot be used for regulatory purposes.

The limited use obligation does not change ASD's ACSC's ability to provide confidential technical guidance, advice and assistance. What it does is give industry assurance that information reported to ASD's ACSC cannot be admitted as evidence in criminal or civil proceedings against them.

ASD **programs**

- ASD's ACSC provides trusted advice and expertise to government, business and the community, drawing on our deep technical understanding of communications technology to help Australians understand the cyber threat environment and what they can do to protect themselves. When serious cyber incidents occur, ASD's ACSC leads the Australian Government's response to help mitigate the threat and strengthen defences.
- ASD's ACSC does not and cannot operate effectively on its own. To protect the nation, ASD's ACSC works with federal and state governments, international counterparts, and industry partners to identify and disrupt malicious cyber threats.
- Partnerships underpin ASD's ACSC's ability to track, detect and mitigate cyber threats and uplift networks that are less prepared. This uplift includes enabling others to defend their own networks, informed by our unique threat insights and partnerships.

Proactive notifications to potential victims

ASD's ACSC uses its unique intelligence insights, international partnerships and industry engagements to identify and share cyber security threats and vulnerabilities to protect Australian organisations.

ASD's ACSC engages with entities when it becomes alerted to a potential vulnerability or an incident that may be affecting an organisation and is often severe in nature. In FY2024–25, ASD's ACSC made more than 1700 notifications to entities of potentially malicious cyber activity, an increase of 83% from FY2023–24.

More than 12% of ASD's ACSC's proactive engagements were confirmed as incidents where some sort of network compromise had occurred. Nearly half (46%) of those incidents were associated with either malware or ransomware, and a further 12% were the result of an observed data breach.

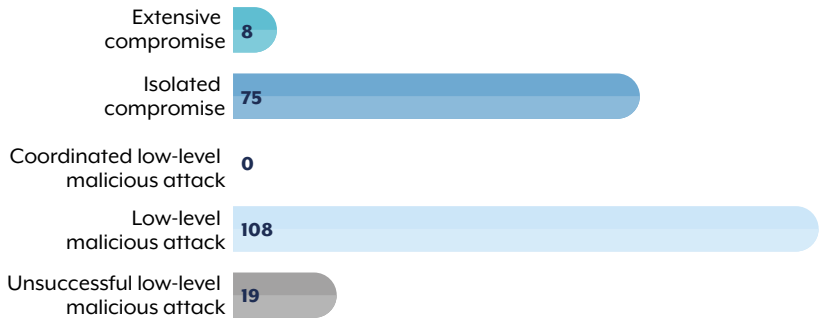


Figure 14: Proactive engagements by ASD's ACSC by severity of incident

Partnership and collaboration with ASD's ACSC

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

In FY2024–25 ASD's Cyber Security Partnership Program grew to over 133,000 partners. ASD's ACSC briefed board and executive leadership team representatives from 41% of the ASX100.

ASD's Cyber Security Partnership Program is a national program delivered through ASD's State Offices, located around Australia. It enables eligible Australian organisations to engage with ASD 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 National Exercise Program (NEP) helps CI and government organisations validate and strengthen Australia's nationwide cyber security arrangements. The program uses exercises and other readiness activities that target strategic decision-making as well as operational and technical capabilities.

Highlight 9: 2024 ASD's ACSC Cyber Drill for ASD's ACSC network partners

In 2024, the NEP delivered the inaugural ASD's ACSC Cyber Drill. This provided an opportunity for ASD's ACSC network partner cyber defence teams to gain valuable hands-on experience detecting and responding to cyber incidents, simulating the TTPs of real-world malicious cyber actors. The ASD's ACSC Cyber Drill was run via a cyber range for technical teams from across key CI sectors and included:

- 25 teams competing in up to 3 knockout rounds
- teams completing a Live Fire Exercise (LFE) each round
- LFEs covering 52 different MITRE ATT&CK techniques
- teams progressing to the next round based on their LFE scores and completion times.

The ASD's ACSC Cyber Drill exercised the technical capabilities of ASD's ACSC network partners, enhancing their ability to detect and respond to malicious cyber activity at speed. The team-based approach to the ASD's ACSC Cyber Drill promoted collaboration and capability enhancement, and enabled cyber security teams to rehearse and improve their responses to cyber incidents while using a virtual environment designed to mirror a corporate network, complete with a range of common industry security tools.

> *Cyber threats are constantly evolving, and so must our readiness. Mastercard welcomes exercises involving government and private sector partnership, collaboration and sharing of best practices.*
>
> *The ASD Cyber Drill is a prime example of this and is critical to ensuring we're prepared to respond swiftly and effectively as a nation. They allow Australia to test its defences, strengthen our cyber security ecosystem coordination, and reinforce our commitment to protecting Australians from malicious cyber activity in both the public and private sectors.*
>
> **– Mastercard**

The Government Uplift Program assists prioritised government entities to strengthen their cyber defences through a range of targeted activities. It delivers hands-on technical assessments of an entity's environments and systems to determine the effectiveness of both prevention and detection security controls as well as also uplift Essential Eight maturity.

Explainer 2: Microsoft-ASD E5 Uplift Program

The Microsoft-ASD Cyber Shield (MACS) partnership is an example of the importance of collaboration between the public and private sectors in countering the cyber threats we collectively face. One of the projects delivered under MACS in the reporting period was the Microsoft 365 E5 Uplift pilot project. ASD's operational experience had found that many federal government organisations subscribed to an E5 licence, but either did not use or had not optimised existing security products within the licence. Between October 2024 and March 2025, ASD partnered with Microsoft to uplift Microsoft Defender for Identity and Microsoft Defender for Endpoint products and configurations for seven government organisations.

Through this project, ASD was able to increase visibility of over 38,000 accounts and enable the identification of 35 previously unidentified vulnerabilities. Additionally, four workshops with over 300 participants across 33 government organisations were delivered to share technical expertise. Learnings from the collaboration have now also been included in ASD's Secure Blueprint for Cloud, which is available at blueprint.asd.gov.au.

Privileged User Training (PUT) offers government and CI privileged users an overview of the best practices in cyber security. Attendees acquire practical knowledge on hacker tools and techniques, learn to manage cyber security risk within an enterprise setting, and explore approaches to cultivating a positive security culture. Most importantly, the course delves deeply into how privileged users can implement tactics to reduce the occurrence of cyber security incidents in their daily work. At the end of FY2024–25, PUT had been delivered to approximately 7,500 participants across 460 entities.

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 critical infrastructure assets and OT environments. A voluntary, nationwide threat-driven program, CI-UP focuses on improving CI's 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 cyber threat landscape in OT in a neutral and trusted environment
- **CI-UP presentations, briefings and workshops** – providing sector-specific insights and trends across a range of CI partners.

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 partnered with the Department of Home Affairs to align its existing bodies of work on threat sharing and threat blocking, using ASD's ACSC's capabilities to provide the back bone of the Threat Blocking and Threat Sharing Scheme. ASD's ACSC leveraged the capabilities of banks and telecommunication providers to block cyber threats at scale, protecting Australians and Australian infrastructure. ASD's CTIS has bridged the gap between intelligence generation and the disruption of malicious infrastructure. Using CTIS, ASD's collaboration with government and industry has managed to block hundreds of malicious websites to date, making the internet a safer place for all Australians.

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 the area of 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.

Case study 2: CHIPs notify a major CI provider of a critical vulnerability

In the final quarter of 2024, an edge device vendor notified ASD's ACSC of a critical vulnerability in one of their products, which had been observed undergoing limited exploitation globally. The vendor requested assistance in reaching Australian operators of those devices.

Through the CHIPs program, ASD's ACSC identified hundreds of entities using the vulnerable device on the Australian internet and notified them about the vulnerability so that they could take action to secure their installations.

One entity, a major CI provider, advised ASD's ACSC that they had patched their system based on the alert received and had then observed malicious cyber actors unsuccessfully attempting to exploit their system within 48 hours.

Reducing the overall internet-facing attack surface, and patching internet-facing systems quickly when critical vulnerabilities emerge, remain key strategies for preventing malicious cyber intrusion.

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 serves 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.

Glossary

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