



Australian Government  
Australian Signals Directorate

**ASD** AUSTRALIAN SIGNALS DIRECTORATE  
**ACSC** Australian Cyber Security Centre

# Annual Cyber Threat Report

2023–2024

## **Website**

[www.cyber.gov.au](http://www.cyber.gov.au)

## **Contact us**

ASD welcomes feedback to improve the services it provides to Australians.

Feedback can be provided by emailing [asd.assist@defence.gov.au](mailto: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**

© Commonwealth of Australia 2024

With the exception of the Coat of Arms, the entity's logo, third party content and where otherwise stated, all material presented in this publication is provided under a Creative Commons Attribution 3.0 Australian Licence. To the extent that copyright subsists in a third party, permission will be required by a third party to reuse the material.

Creative Commons Attribution 3.0 Australia Licence is a standard form licence agreement that allows you to copy, distribute, transmit and adapt this publication provided that you attribute the work.

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

The Commonwealth's preference is that you attribute this publication (and any material sourced from it) using the following wording: © Commonwealth of Australia 2024, Australian Signals Directorate, 2023–24 Annual Cyber Threat Report.

## **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](http://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

2023-2024



# Foreword

I am pleased to present the 2023–24 Annual Cyber Threat Report.

This year’s report comes amid a continued deterioration in Australia’s strategic environment. The Indo-Pacific continues to face entrenched strategic competition, Russia’s invasion of Ukraine has entered its third year and conflict continues to unfold in the Middle East.

As the 2024 National Defence Strategy outlined, these challenges are being compounded by rapid technological advancements. Malign actors – both state and non-state – are improving their cyber capabilities, increasing the risk of disruptions to Australia’s critical systems, infrastructure and networks. Grey-zone activities have also expanded in the Indo-Pacific, with malicious cyber actors continuing to conduct espionage and spread disinformation.

This year’s report outlines the cyber threat posed to Australian governments, critical infrastructure, businesses and households. It shows how malicious state actors and cybercriminals are continuing to adapt their tradecraft in an attempt to compromise Australian networks.

These circumstances underline the significant role that cyber capabilities play in safeguarding our national security and the critical role ASD continues to play in protecting Australians. That is why the Albanese Government has committed \$15–\$20 billion to 2033–34 to enhance our cyber domain capabilities as part of the 2024 Integrated Investment Program.

This significant investment will provide greater visibility of threats to critical infrastructure, increase the resilience of our infrastructure to cyber attacks, provide new intelligence functions and enable offensive cyber operations. The Government has also prioritised REDSPICE funding to enhance ASD’s signals intelligence and cyber capabilities.

This report highlights the importance of strong partnerships between the public and private sectors in defending Australians from cyber threats and making our country a harder target. It also reflects the concrete steps we are taking to deter cybercriminals and hold them to account, with the Government having used for the first time Australia’s autonomous cyber sanctions framework to impose cyber sanctions on Russian cybercriminals.

Informed by ASD’s intelligence insights and partnerships, this report reinforces the importance of enhancing our nation’s cyber defences and the need for all Australians to play their part in protecting our collective cyber security. Reporting cybercrime, incidents and vulnerabilities remains a critical part of building a national threat picture and enabling us to effectively counter malicious cyber actors.

This report is a key part of the Government’s efforts to raise the profile of Australia’s cyber threats to ensure we can respond effectively to keep Australians safe.



**The Hon Richard Marles MP**

Deputy Prime Minister and Minister for Defence



# Contents

<b>About ASD's ACSC</b> .....	viii
<b>About the contributors</b> .....	viii
<b>Executive summary</b> .....	1
<b>Year in review</b> .....	3
<b>State actors</b> .....	13
<b>Critical infrastructure</b> .....	19
<b>Cybercrime</b> .....	29
<b>Hacktivism</b> .....	45
<b>Resilience</b> .....	47
<b>ASD programs</b> .....	59

## 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 119,300 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 thanks all of 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.

## 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 and the AFP to disrupt the most serious cybercrime threats facing Australia. The AFP-led Joint Policing Cybercrime Coordination Centre (JPCC3) brings together Australian law enforcement and key industry and international partners to fight high-volume, high-harm cybercrime and prevent harm and financial loss to 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 includes intelligence collection, investigations and intelligence-led outreach to business and government partners.



Australian Government  
Department of Foreign Affairs and Trade

## 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 Cyber Security Strategy, the development of which is being coordinated by the Department of Home Affairs.



Australian Government  
Department of Home Affairs

## Department of Home Affairs

The Department of Home Affairs is responsible for central coordination, strategy and policy leadership of cyber and critical infrastructure resilience and security, immigration, border security, national security and resilience, counter-terrorism, and citizenship. The Department of Home Affairs leads the development of cyber security policy, including the implementation of the *2023–2030 Australian Cyber Security Strategy*.



Australian Government  
National Cyber Security Coordinator

## 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 National AntiScam 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 collaboration (technology and intelligence sharing), disruption, awareness and protection.



## Defence Intelligence Organisation

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



Australian Government  
Office of the Australian Information Commissioner

## 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.



RESERVE BANK  
OF AUSTRALIA

## Reserve Bank of Australia

The Reserve Bank of Australia is Australia's central bank. Its duty is to serve the Australian people and contribute to their economic prosperity and welfare through sustainment of full employment and maintenance of price stability. It issues the nation's banknotes and operates the core of the payments system.

# Executive summary

Australia faces the most complex and challenging strategic environment since the Second World War. These strategic challenges extend to the cyber threat landscape. While advancements in critical and emerging technologies offer significant social and economic benefits, they also improve the capabilities of malicious cyber actors who continue to target Australia's networks.

In FY2023–24, ASD received over 36,700 calls to its Australian Cyber Security Hotline, an increase of 12% from the previous financial year. ASD also responded to over 1,100 cyber security incidents, highlighting the continued exploitation of Australian systems and ongoing threat to our critical networks.

State-sponsored cyber actors persistently target Australian governments, critical infrastructure and businesses using evolving tradecraft. These actors conduct cyber operations in pursuit of state goals, including for espionage, in exerting malign influence, interference and coercion, and in seeking to pre-position on networks for disruptive cyber attacks.

Over the past year, ASD co-sealed several joint advisories with international partners to highlight the evolving operations of state-sponsored cyber actors. In February 2024, ASD joined the US and other international partners in releasing an advisory that assessed the People's Republic of China (PRC) is leveraging living off the land techniques that abuse native tools and processes on systems. The PRC's choice of targets and pattern of behaviour is consistent with pre-positioning for disruptive effects rather than traditional cyber espionage operations.

Russia is also adapting its techniques, including for the exploitation of cloud platforms. The evolution of this tradecraft means that network defenders must prioritise and invest in cyber security skills, resources and teams.

Critical infrastructure networks are an attractive target due to the sensitive data they hold and the widespread disruption that a cyber security incident can cause on those networks. In FY2023–24, over 11% of cyber security incidents ASD responded to related to critical infrastructure. Compromise could lead to the disruption of critical services, affecting the economy and lives of everyday Australians.

Cybercrime is a persistent and disruptive threat. Cybercriminals are adapting to capitalise on new opportunities, such as artificial intelligence, which reduces the level of sophistication needed for cybercriminals to operate. In FY2023–24, business email compromise and fraud were among the top self-reported cybercrimes for businesses and individuals in Australia. Ransomware and data theft extortion also remained a pervasive and costly threat.

In response to this threat, ASD has worked across government, with industry and international partners to successfully pursue cybercriminals targeting Australia. During FY2023–24, the Australian Government for the first time used Australia's autonomous cyber sanctions framework to sanction two Russian citizens for their roles in cybercrime activities. These sanctions are a key tool in deterring cybercrime and protecting Australians.



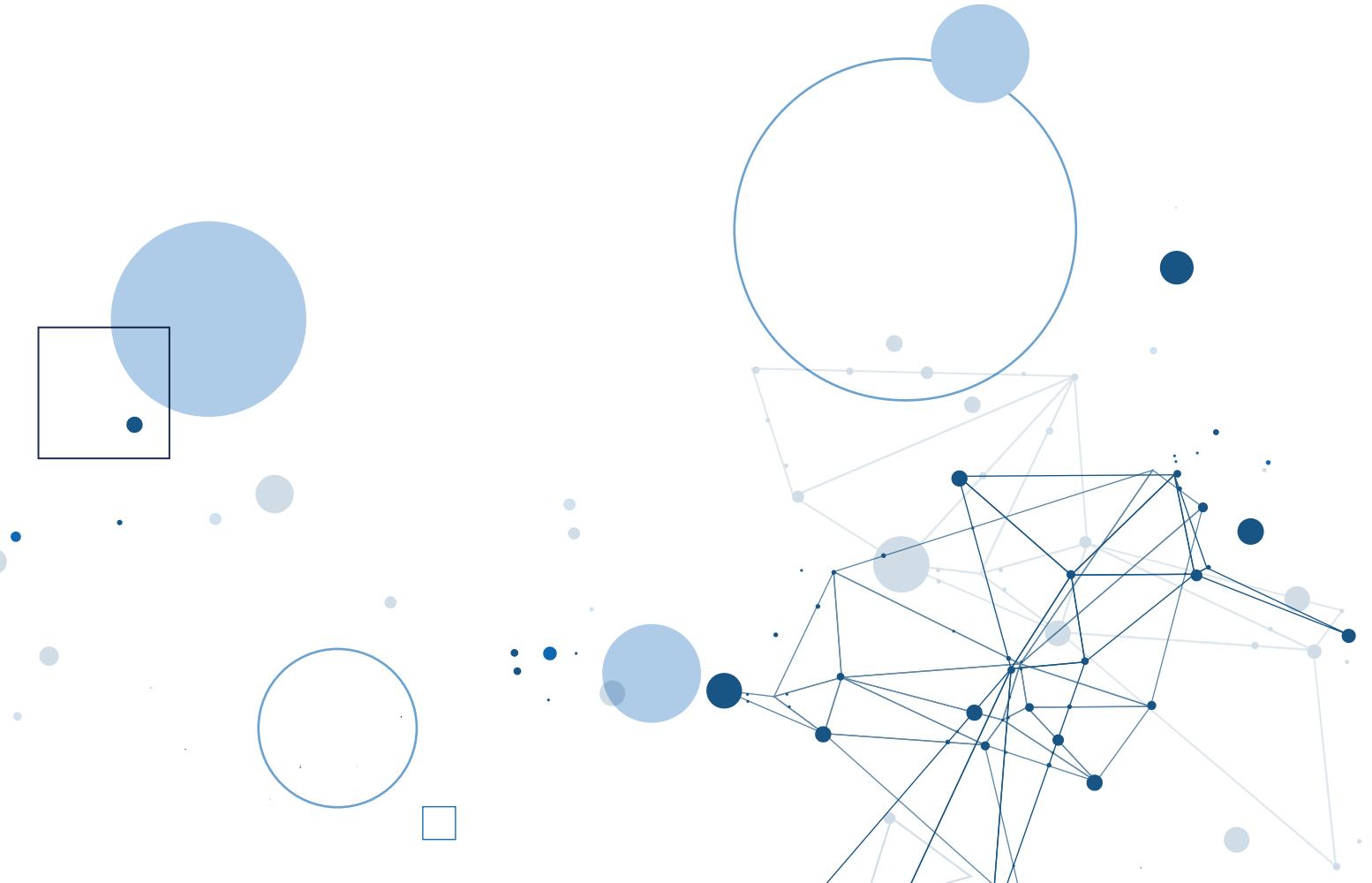
Strong partnerships are critical to building cyber resilience and making Australia a harder target. ASD continues to monitor and adapt to the threat environment, and collaborates on a national scale to protect Australians. An increasing number of industry and government partners are choosing to participate in ASD programs, which provide a platform to share threat intelligence and expertise. This includes the ASD-Microsoft initiative to connect ASD's Cyber Threat Intelligence Sharing platform with Microsoft's Sentinel platform. These types of collaborations are improving the speed and scale of information-sharing between and among government agencies and industry partners.

In FY2023–24, ASD notified entities more than 930 times of potential malicious activity on their networks. A robust partnership between government and industry underpins our ability to effectively defend the nation against malicious cyber activity.

Cyber security is not set-and-forget. Organisations should consider replacing unsupported information and communications technology (ICT) systems with secure-by-design products, consider cyber security when implementing new technologies and follow ASD's best-practice cyber security advice, such as the Essential Eight. Regularly updating and applying ICT best practice builds resilience now and into the future.

Be ready to respond. Critical infrastructure organisations should adopt a stance of 'when' not 'if' a cyber security incident will occur. All organisations should have a cyber security incident response plan and test it regularly to ensure an effective response and fast recovery. To develop and implement a response plan, an organisation needs to know its systems and where its most valuable data is stored.

ASD encourages every organisation and individual who observes suspicious cyber activity, incidents and vulnerabilities to report to ReportCyber at [cyber.gov.au](https://cyber.gov.au), and to the Australian Cyber Security Hotline 1300 CYBER1 (1300 292 371). ASD provides free technical incident response advice and assistance, 24 hours a day, 7 days a week.



# YEAR IN REVIEW

## What ASD saw



Answered over **36,700** calls to the Australian Cyber Security Hotline, **up 12%**

- on average, **100 calls per day**, an increase from **90 calls per day**



Average self-reported cost of cybercrime per report for individuals, **up 17%** (\$30,700)

Average self-reported cost of cybercrime per report for businesses, **down 8%** overall

- small business: **\$49,600** (up 8%)
- medium business: **\$62,800** (down 35%)
- large business: **\$63,600** (down 11%)



Received over **87,400** cybercrime reports, **down 7%**

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



### **Top 3 self-reported cybercrime types for individuals**

- identity fraud (26%)
- online shopping fraud (15%)
- online banking fraud (12%)



### **Top 3 self-reported cybercrime types for business**

- email compromise (20%)
- online banking fraud (13%)
- business email compromise fraud (13%)



Publicly reported common vulnerabilities and exposures  
**increased 31%**



**11%** of all incidents  
responded to included **ransomware**,  
a **3% increase** from last year

# YEAR IN REVIEW

## What ASD did



Responded to over  
**1,100 cyber security incidents**,  
*similar to last year*



Notified entities **930** times of  
**potential malicious cyber activity**



**Australian Protective Domain Name System**  
blocked customer access to **82 million** malicious domains,  
**up 21%**



**Domain Takedown Service**  
has requested the removal of **over 189,000**  
malicious domains targeting Australian servers,  
**up 49%**



### Cyber Threat Intelligence Sharing partners

grew by **66%** to over **400 partners**

- shared over **1,372,400 indicators of compromise**



### Cyber Hygiene Improvement Program

- performed **365** high-priority operational taskings,  
**up 250%**
- distributed around **6,400** reports  
to approximately **2,000** organisations,  
up **32%** and **48%** respectively



### Cyber Uplift Remediation Program

- **24** active engagements
- **17** engagements commenced

### Cyber Maturity Measurement Program

- **16** active engagements

# YEAR IN REVIEW

## What ASD did



### Critical Infrastructure Uplift Program

- **10** uplifts completed covering **15 CI assets**
- **5** uplifts in progress
- **17** uplift information packs sent
- **42** uplift workshops held



Notified critical infrastructure organisations  
**over 90 times** of potential malicious cyber activity



Published or updated **29 PROTECT** publications,  
updated the **Information Security Manual**  
quarterly, and updated the **Essential Eight**  
**Maturity Model**



Published **19 joint advisories and publications**  
with international partners to cyber.gov.au



Published **118 alerts, advisories, incident and insight reports** on **cyber.gov.au** and the **Partnership Portal**



**ASD's Cyber Security Partnership Program** grew to around **119,300 partners**

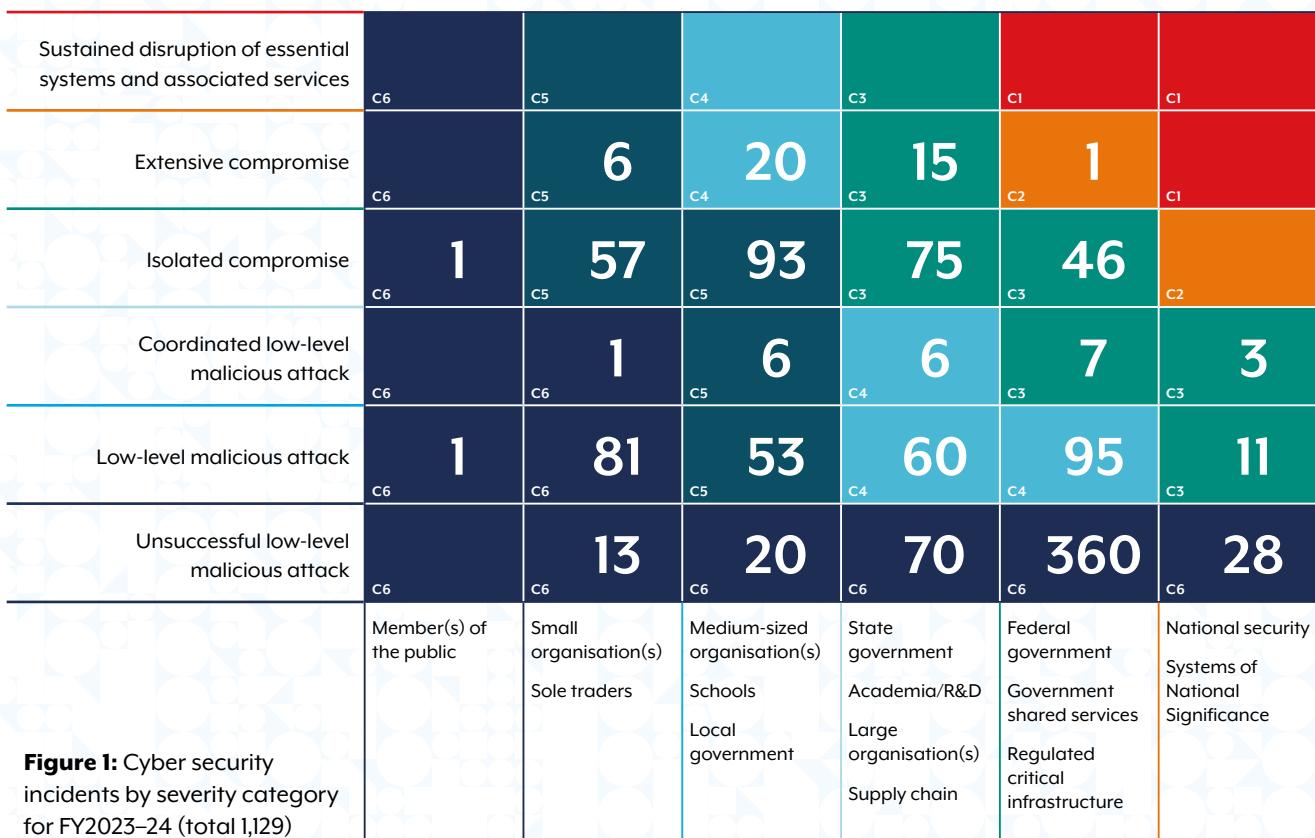


Led **16 cyber security exercises** involving over **130 organisations** to strengthen Australia's cyber resilience



Briefed board members and company directors covering **37%** of the ASX200

# YEAR IN REVIEW



ASD 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.

In FY2023–24, there was a slight decrease in the number of extensive compromises, while the number of unsuccessful low-level malicious attacks increased by 10% compared with FY2022–23. There was also a 39% increase in isolated compromises this financial year.

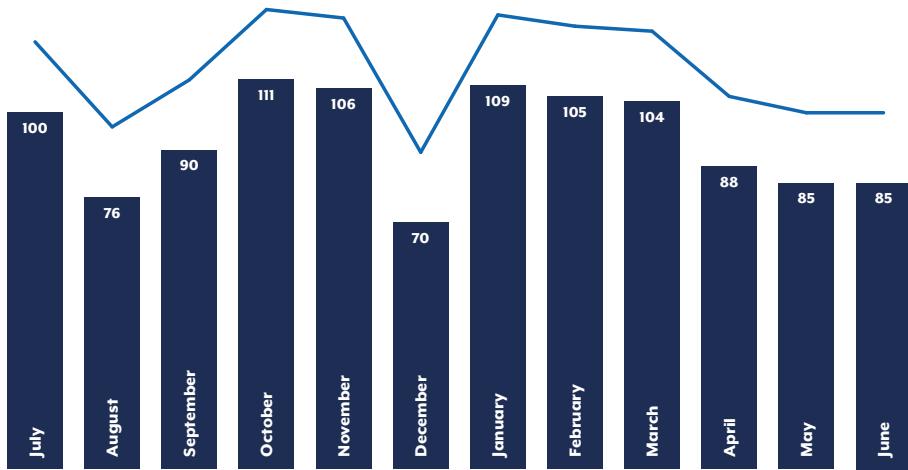
Coordinated low-level malicious cyber attacks fell by 77%, however this largely reflects a spike in incidents in FY2022–23 following a specific hacktivist campaign. It does not necessarily imply that the threat of coordinated low-level malicious cyber activity has diminished.

Incidents categorised as C3 or above involve organisations such as federal and state governments, large organisations, academia, and supply chains. The frequency of C3 or above incidents in FY2023–24 was consistent with FY2022–23, with 14% of all incidents being categorised C3 or above. While ASD only responded to one C2 incident, down from 5 in FY2022–23, the nature of the incident highlights the importance of ensuring systems are updated – the C2 was through the exploitation of a known vulnerability targeting a legacy, unpatched test server.

Over a quarter (26%) of all C3 incidents were discovered as a result of a tipper, where ASD proactively notified the affected organisation of suspicious activity. The most common malicious activity leading to 30% of C3 incidents was the exploitation of public facing applications.

C3 incidents commonly involved compromised accounts or credentials (23%), malware infection other than ransomware (19%) and compromised assets, networks or infrastructure (18%). This contrasts with C3 incidents in FY2022–23, where assets, networks or infrastructure were more frequently compromised than accounts or credentials. This suggests that malicious actors will adapt their methods to gain access.

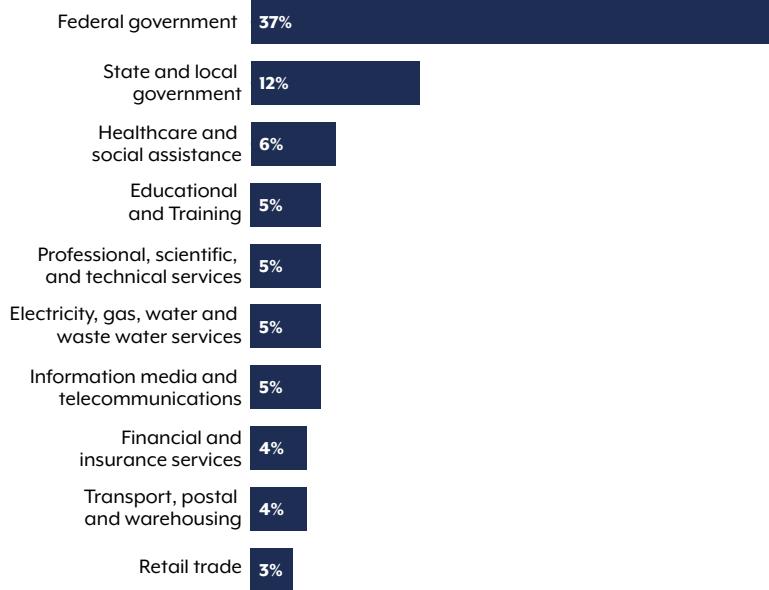
ASD responded to **over 1,100 cyber security incidents**, around the same as in the last financial year.



**Figure 2:** Cyber security incidents by month

## The top 5 reporting sectors are consistent with FY2022–23.

ASD categorises sectors following the Australian and New Zealand Standard Industrial Classification Divisions from the Australian Bureau of Statistics. The public safety and administration division encompasses several sectors, including federal, state, territory and local governments, public order and safety services, and defence.



**Figure 3:** Top 10 reporting sectors

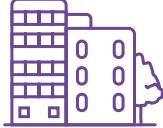
Compared to FY2022–23, healthcare and social assistance rose to be the most frequently reported non-government sector.

Government sectors and regulated critical infrastructure have additional reporting obligations, which may explain the relatively high reporting rate for these sectors compared with others.

- The number of extortion-related cyber security incidents responded to by ASD increased by 9% compared to the last financial year.
  - Around 71% of these incidents involved ransomware.
- In FY2023–24, ASD responded to 53 incidents involving Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks, a decrease of 15% on the last financial year.

# Reported top 3

Cyber security incident types	Mitigations
<b>Top 3 reported cyber security incident types for critical infrastructure</b> 	<ul style="list-style-type: none"> <li>■ Use phishing-resistant multi-factor authentication (MFA) where possible</li> <li>■ Analyse event logs from workstations in a timely manner to detect cyber security events</li> <li>■ Find and remove inactive user and service accounts</li> <li>■ Enforce the principle of least privilege</li> </ul>
	<ul style="list-style-type: none"> <li>■ Use antivirus software and endpoint detection and response software</li> <li>■ Keep your devices up to date</li> <li>■ Implement application control</li> <li>■ Maintain backups of critical data applications and settings. Regularly test that you can restore from backups in a timely manner</li> </ul>
	<ul style="list-style-type: none"> <li>■ Use network segmentation and segregation</li> <li>■ Apply ASD's <i>industrial control systems remote access protocol</i></li> <li>■ Define a process for introducing software and patches into the industrial control system</li> <li>■ Ensure sufficient logging is enabled and monitor for key indicators</li> <li>■ Ensure logs are stored securely</li> </ul>
Cyber security incident types	Mitigations
<b>Top 3 reported cyber security incident types for government (federal, state and local)</b> 	<ul style="list-style-type: none"> <li>■ Use phishing-resistant MFA where possible</li> <li>■ Use a password management solution to store passwords securely</li> <li>■ Ensure event logs from authentication services and workstations are analysed within a timely manner to detect cyber security events</li> </ul>
	<ul style="list-style-type: none"> <li>■ Mitigate known vulnerabilities (e.g. applying patches in a timely manner)</li> <li>■ Implement access control and application control</li> <li>■ Use antivirus software and endpoint detection and response software</li> <li>■ Maintain backups of critical data applications and settings. Regularly test that you can restore from backups in a timely manner</li> </ul>
	<ul style="list-style-type: none"> <li>■ Use system and application hardening</li> <li>■ Adopt a Secure-by-Design approach</li> <li>■ Apply network access controls</li> <li>■ Ensure logging is enabled and monitor for key indicators</li> </ul>

Self-reported cybercrime types	Mitigations
Email compromise resulting in no financial loss <b>20%</b>	<ul style="list-style-type: none"> <li>■ Train staff to recognise phishing which is commonly used to compromise accounts</li> <li>■ Require MFA and strong, unique passwords for business email accounts</li> <li>■ Use email content filtering</li> </ul>
<b>Top 3 self-reported cybercrime threats for business (S,M,L)</b> 	<ul style="list-style-type: none"> <li>■ Be aware of suspicious changes to banking details or payment requests</li> <li>■ Be aware of changes to email addresses – such as if the domain name does not match the supplier's company name or differs from previous correspondence</li> <li>■ Be aware of unsolicited SMS messages from financial providers – including messages that ask for a password, an MFA code, or to click on a link</li> </ul>
Business email compromise (BEC) fraud resulting in financial loss <b>13%</b>	<ul style="list-style-type: none"> <li>■ Increase cyber security awareness training for staff</li> <li>■ Use MFA for identity confirmation</li> <li>■ Protect domain names – renew domain names on schedule and register additional domain names</li> </ul>
Self-reported cybercrime types	Mitigations
<b>Top 3 self-reported cybercrime threats for individuals</b> 	<ul style="list-style-type: none"> <li>■ Use MFA and secure passphrases</li> <li>■ Keep your devices up to date and use antivirus software</li> <li>■ Limit the personally identifiable information you share online</li> </ul>
Identity fraud <b>26%</b>	<ul style="list-style-type: none"> <li>■ Use MFA and secure passphrases</li> <li>■ Keep your devices up to date and use antivirus software</li> <li>■ Limit the personally identifiable information you share online</li> </ul>
Online shopping fraud <b>15%</b>	<ul style="list-style-type: none"> <li>■ Use MFA and secure passphrases</li> <li>■ Keep your devices up to date and use antivirus software</li> <li>■ Limit the personally identifiable information you share online</li> </ul>
Online banking fraud <b>12%</b>	<ul style="list-style-type: none"> <li>■ Use MFA through your financial providers</li> <li>■ Be aware of suspicious changes to banking details or payment requests</li> <li>■ Be aware of changes to email addresses – such as if the domain name does not match the supplier's company name or differs from previous correspondence</li> <li>■ Be aware of unsolicited SMS messages from financial providers – including messages that ask for a password, an MFA code, or to click on a link</li> </ul>

**Figure 4:** Most common reported threats and key steps to improving cyber security

Note: Incidents can have multiple incident types.

For best-practice cyber security mitigation advice, including ASD's Essential Eight, visit [cyber.gov.au](http://cyber.gov.au).

# Chapter 1



## State actors

- The threat of state-sponsored cyber operations is persistent and will likely grow as strategic competition in the Indo-Pacific increases.
- State-sponsored cyber actors will continue targeting Australian governments, critical infrastructure, and businesses, as well as connected systems and their supply chains, for espionage and information-gathering purposes. These actors will continue to adapt their techniques, using both publicly available and bespoke tools to achieve their objectives.
- In February 2024, ASD joined other Five Eyes partners in a US-led advisory, which assessed that the People's Republic of China state-sponsored cyber actors are seeking to pre-position themselves on information and communications technology networks for disruptive cyber attacks against US critical infrastructure in the event of a major crisis or conflict. Australian critical infrastructure networks could be vulnerable to similar state-sponsored malicious cyber activity as seen in the US.
- ASD's Cyber Security Partnership Program and the Cyber Threat Intelligence Sharing platform support Australian organisations to combat state-based cyber threats.

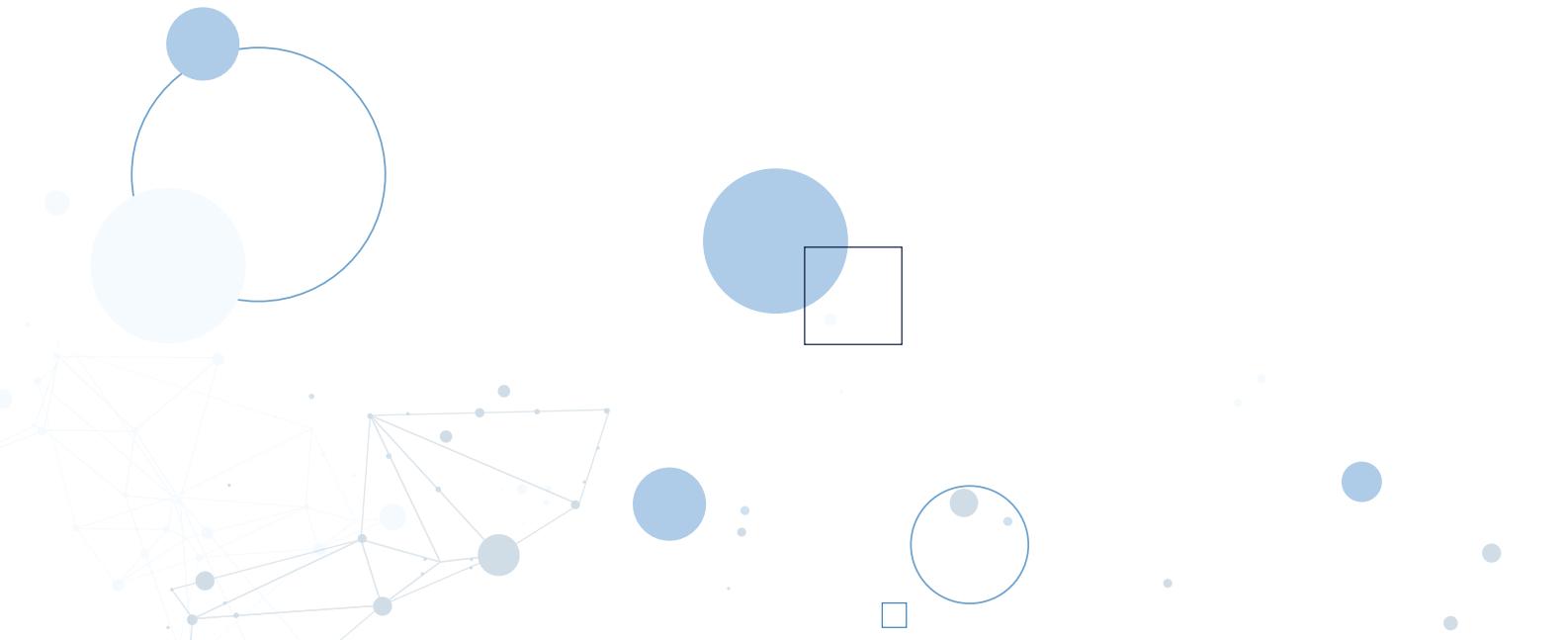
# Global state-sponsored cyber activity increases as tensions rise

Australia continues to face a complex set of strategic circumstances. Multiple ongoing conflicts are fueling international instability and increasing strategic competition between the US and China is a primary feature of our security environment.

## Explainer 1: Australia's strategic environment

The 2024 National Defence Strategy highlights that Australia faces its most complex and challenging strategic environment since the Second World War. Entrenched and increasing strategic competition is being accompanied by an unprecedented conventional and non-conventional military build-up in our region, without strategic reassurance or transparency. Grey-zone activities have also expanded in the Indo-Pacific and are facilitated by technological developments, including in cyber capabilities. Threats posed by state and non-state actors in the cyber domain are multiplying.

State-sponsored cyber operations continue to play a significant role in this strategic environment. State-sponsored cyber actors gather intelligence, exert malign influence, interference and coercion, and seek to pre-position on critical networks. In the event of a major deterioration in the strategic environment, Australia could be the target of significant disruptive cyber activities.



## Cyber attacks in modern conflict

Russia's invasion of Ukraine and the Israel-Hamas conflict both offer contemporary examples of how cyber operations can support military and strategic objectives in conflict.

Since the beginning of Russia's invasion of Ukraine, cyber attacks have been used to cause disruptive and destructive effects to both military and civilian infrastructure, including on telecommunications organisations, postal and energy systems, and governments. These attacks have resulted in mobile and fixed-line communications outages and blackouts that have impacted military operations and civilian populations.

Conflict can also give rise to politically-motivated cyber activity. During the Israel-Hamas conflict, patriotic hacking – a type of politically-motivated cyber activity – has been reported on both sides of the conflict, with varying degrees of severity. This includes critical infrastructure targeting, digital billboard and website defacement, and Distributed Denial of Service attacks.



# The threat of state-sponsored cyber operations in Australia

State-sponsored cyber actors will continue targeting Australian governments, critical infrastructure and businesses.

Australian networks – particularly those connected to critical infrastructure systems either directly or through their supply chains – may be targeted in order to pre-position capabilities for disruptive effects, or may be used to access a higher-value target network.

State-sponsored cyber actors also have information-gathering and espionage objectives in Australia. State actors have an enduring interest in obtaining sensitive information, intellectual property and personally identifiable information to gain strategic and tactical advantage. Australian organisations often hold large quantities of data, so are likely a target for this type of activity.

State-sponsored cyber actors often use previously stolen data, including from previous Australian cyber security incidents (such as network information and credentials) to further their operations and re-exploit network devices. 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 their use of similar techniques and weaknesses in systems.

## Tools and techniques of state-sponsored cyber actors

State-sponsored cyber actors use various tools and techniques to avoid detection and achieve their objectives. These tools can be advanced and bespoke. However, they also use common, simple tools and techniques to prevent the discovery of their best cyber capabilities.

### Case study 1: Simple techniques can be effective for state aims

In December 2023, ASD and international partners released an advisory detailing a global spear phishing campaign conducted by a Russian Federal Security Service (FSB) actor, Star Blizzard. The FSB-sponsored group targeted a number of sectors – including defence, government, academia, and think tanks – around the world.

Spear phishing is an effective but simple technique used by many different cyber actors. The advisory highlights that techniques do not need to be advanced for state actors to achieve their goals.

The advisory, *Russian FSB cyber actor Star Blizzard continues worldwide spear phishing campaigns*, is available at [cyber.gov.au](https://cyber.gov.au).

## Supply chain compromises

State-sponsored cyber actors can compromise target networks via their supply chains. The Australian Government has previously attributed supply chain targeting to state-sponsored cyber actors, including Russian actors that targeted US software firm SolarWinds.

Cyber supply chain risk management should form a significant component of an organisation's overall cyber security strategy. An effective strategy includes consideration of the product or service's design, manufacture, delivery, maintenance, decommissioning, and disposal. On 22 May, 2024 ASD released updated advice on how to manage supply chain risks, available on [cyber.gov.au](#).

## Living off the land techniques

State-sponsored cyber actors 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).

FEBRUARY	<p>In <b>February 2024</b>, ASD joined the US and other international partners in releasing an advisory, <i>PRC state-sponsored actors compromise and maintain persistent access to US critical infrastructure</i>. The US assessed that PRC state-sponsored cyber actors had compromised and maintained access to US critical infrastructure networks for disruptive cyber attacks in the event of a major crisis or conflict. US agencies also assessed with high confidence that PRC state-sponsored cyber actor Volt Typhoon, was pre-positioning itself on information and communications technology (ICT) networks to enable lateral movement to operational technology (OT) assets to disrupt functions. In the advisory, ASD assessed Australian critical infrastructure could be vulnerable to similar activity from these actors.</p> <p>Also in <b>February 2024</b>, ASD and international partners released an advisory, <i>Identifying and Mitigating Living Off the Land Techniques</i>, which outlines techniques being deployed by the PRC and Russia to compromise and maintain access to critical infrastructure systems.</p>
MARCH	<p>In <b>March 2024</b>, ASD and international partners released a fact sheet, <i>PRC State-Sponsored Cyber Activity: Actions for Critical Infrastructure Leaders</i>, detailing Volt Typhoon's activities and providing defensive actions for critical infrastructure organisations. The fact sheet made several recommendations, including making informed and proactive resourcing decisions, securing supply chains, and driving a cyber security culture within organisations.</p>

These advisories and fact sheets highlight the threat posed by malicious cyber actors using LOTL techniques to avoid detection and, importantly, the ways in which good cyber security can mitigate the LOTL threat. 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. *Best Practices for Event Logging and Threat Detection* at [cyber.gov.au](#) builds on existing LOTL advice.

## Cloud techniques

As organisations move to cloud-based infrastructure, malicious cyber actors are adapting their techniques to exploit these systems for espionage. Techniques used to access an organisation's cloud services include brute-force attacks and password spraying to access highly privileged service accounts.

In February 2024, ASD and international partners released an advisory detailing the tactics, techniques and procedures used by a Russian state-sponsored cyber actor to gain access to a cloud environment. This group is attributed to the Russian Intelligence Services (SVR) – and known as APT29, Midnight Blizzard, the Dukes, and Cozy Bear. The advisory also outlines the group's previous activity targeting supply chains, demonstrating how tactics, techniques and procedures can evolve as technology changes. The advisory, *SVR cyber actors adapt tactics for initial cloud access*, is available at [cyber.gov.au](https://cyber.gov.au).

## Collaborating to defend Australia's networks

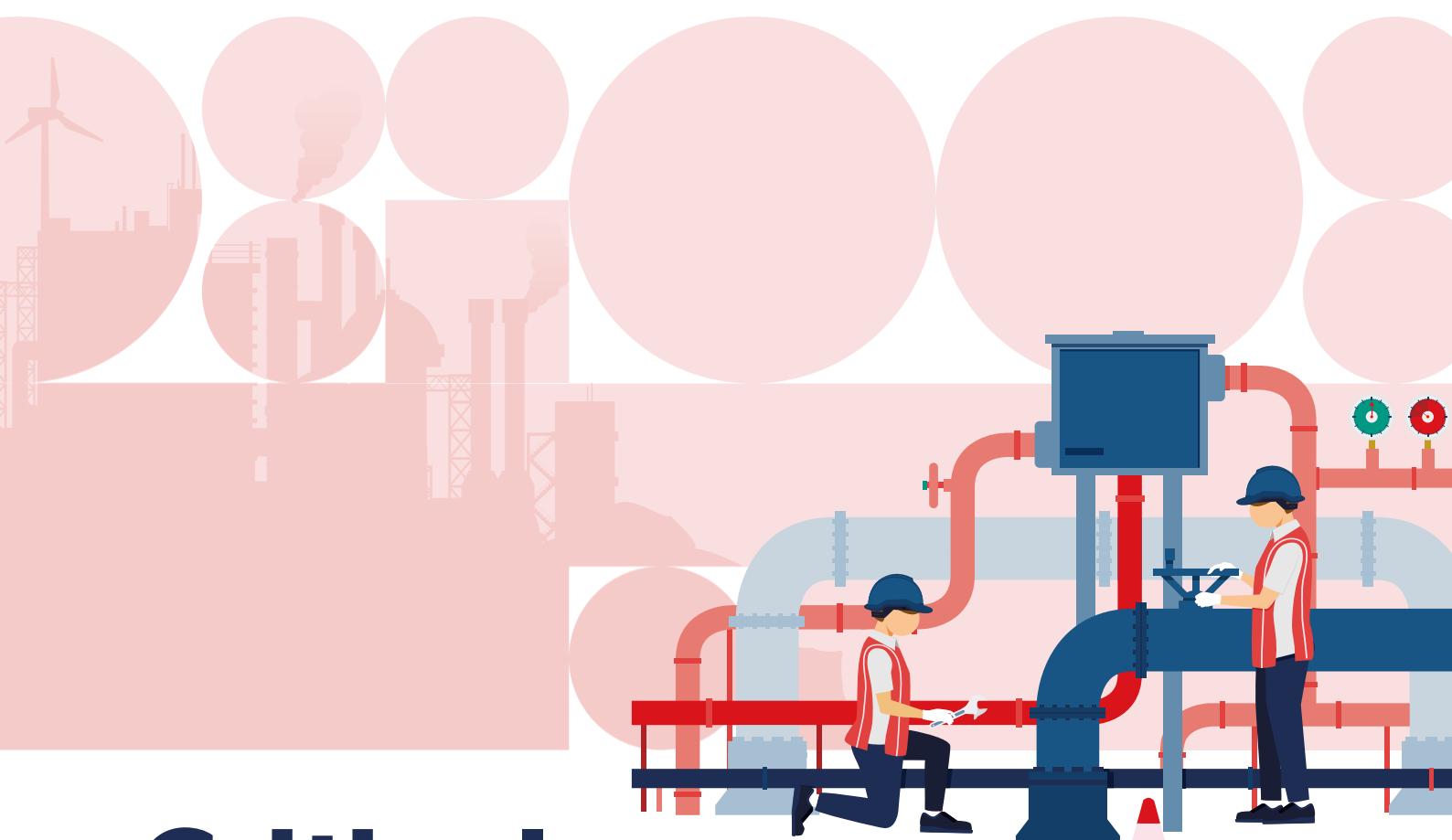
Cyber security collaboration on a national scale is one of Australia's greatest advantages in building resilience against malicious cyber activity. Sharing information and expertise between ASD and industry partners helps to create a collective understanding of this threat and inform new cyber security defences.

The Cyber Threat Intelligence Sharing (CTIS) platform and the ASD's Cyber Security Partnership Program are services that empower Australian organisations to defend their networks and to share the malicious cyber activity they observe. CTIS shares indicators of compromise, bi-directionally at machine speed, within a growing community of Australian government and industry partners, and alerts security operations centre analysts to cyber threats. The ASD's Cyber Security Partnership Program offers opportunities to engage in cyber defence and resilience programs. Participating in these programs strengthens Australia's cyber capabilities to enable intelligence sharing, build the national cyber threat picture and enhance Australia's cyber defences.

ASD encourages all organisations that observe suspicious cyber activity, incidents, and vulnerabilities to report through ReportCyber on [cyber.gov.au](https://cyber.gov.au).



# Chapter 2



## Critical infrastructure

- Australian critical infrastructure organisations are regularly targeted by malicious cyber actors because they provide critical services, hold sensitive data, and are often connected to other critical infrastructure organisations.
- Many different malicious cyber actors target critical infrastructure systems to fulfil their objectives. These include espionage, pre-positioning for disruptive attacks, and for financial gain.
- Operational technology systems are increasingly interconnected and can have vulnerabilities that make them an easier cyber target. Secure information and communications technology and operational technology systems are necessary to protect Australia's critical services.
- Critical infrastructure organisations should adopt a stance of 'when' not 'if' a cyber security incident will occur. Organisations should understand and map their networks, implement an event logging system and maintain an asset registry.

# Critical infrastructure in FY2023–24



Critical infrastructure made up **11%** of all cyber security incidents.



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

- phishing (23%)
- exploitation of a public-facing application (21%)
- brute-force activity (15%).



The **3 most common** cyber security incident types affecting Australian critical infrastructure organisations were:

- compromised account or credentials (32%)
- malware infection (other than ransomware) (17%)
- compromised asset, network or infrastructure (12%).



**Denial of Service** and **Distributed Denial of Service** were overrepresented in critical infrastructure cyber security incidents, and present more than twice as often (11%) when compared to other incidents (5%) responded to by ASD.



The **most frequently reported** critical infrastructure sectors were electricity, gas, water and waste services (30%), education and training (17%) and transport, postal and warehousing (15%).

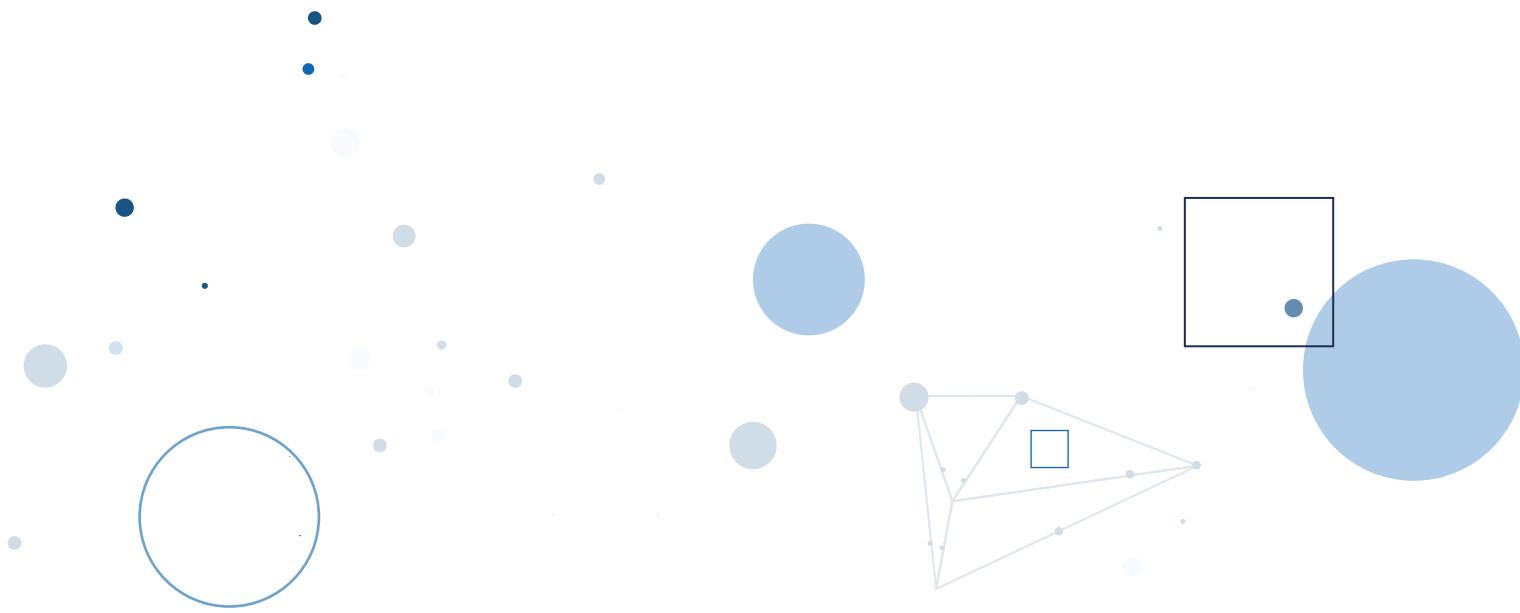
# Malicious cyber activity against critical infrastructure systems is persistent

Critical infrastructure will remain an attractive target for malicious cyber actors because they hold sensitive data and provide essential services that support Australian society. To deliver these services, critical infrastructure organisations often rely on complex networks, supply chains and management solutions. This complexity creates a broad attack surface that malicious cyber actors can exploit.

Operational disruptions to critical infrastructure can be severe and can directly affect the lives of many Australians. For example, prolonged and widespread failure in the energy sector could result in shortages or the disruption of essential medical supplies, instability in the supply of food and groceries, and disrupted telecommunications networks, transport and traffic management systems, and fuel supplies. A compromise could also lead to data breaches containing personal or commercially sensitive information, which in turn could be on-sold or used for other malicious purposes.

Over the past year, malicious cyber actors – including state-sponsored cyber actors, cybercriminals, and hacktivists – have targeted critical infrastructure around the world.

- State-sponsored cyber actors may target critical infrastructure systems for espionage, or to pre-position themselves on networks for future disruptive effects during crises or conflicts.
- Profit-driven cybercriminals may opportunistically target critical infrastructure organisations for financial gain, seeking to extort victims by disrupting critical services or stealing data. Cybercriminals will pressure a victim to pay to restore services and minimise the potential consequences of a cyber security incident – including reputational and financial damage, and potential legal repercussions.
- Hacktivists may disrupt critical infrastructure organisations through low-capability attacks, including website defacement and DDoS attacks. Cyber security incidents affecting critical infrastructure can be high profile – something that may encourage hacktivist activity to elevate their messaging.



## Case study 2: Hospital reports unauthorised access to network

In early 2024, a managed service provider (MSP) discovered unauthorised access to a network belonging to a critical hospital. A hospital employee's personal device had been used to access a Microsoft Azure Virtual Desktop (AVD) environment. Additionally, multi-factor authentication (MFA) controls had been bypassed as the hospital used cached sessions where users were not prompted for MFA for 14 days after a sign-in.

Once in, the malicious cyber actor scanned the network using a non-installer port scanner that did not require administrative privileges to operate, and was allowed to run because application control was not in place. However, the actor was unable to escalate their privileges, and an attempt to download a tool to brute-force passwords was blocked by the proxy server.

The malicious cyber activity triggered an alert in Microsoft Defender, which was investigated by the MSP. The MSP immediately contacted the user to change their password, suspended any active sessions of the compromised user, wiped their AVD instance, and requested the user run anti-malware scans on their personal device.

The MSP identified that the user's personal information may have been compromised in a separate data breach of an unconnected retailer in 2023. The malicious cyber actor capitalised on the exposed details by calling the user – masquerading as an electronic goods retailer – and convincing them to supply their username. The user reported the suspicious call to the MSP scam email reporting facility. However, as it was not an email-based threat it was treated as low urgency and the user was directed to contact the Service Desk.

At no point during the incident was patient care or data impacted and the MSP assessed that no data had been stolen. The hospital and the MSP promptly remediated the incident and worked closely to implement improvements, such as prompting MFA at every login.

The hospital, which is designated under the *Security of Critical Infrastructure Act 2018* (SOCI Act), quickly reported the incident to ASD through its MSP, fulfilling its obligations under the SOCI Act. Furthermore, the hospital shared indicators of compromise (IOCs) with ASD, thereby assisting in the mitigation of similar incidents.

Effective MFA and application control under the Essential Eight would likely have prevented this incident. For more information, see the *Essential Eight Maturity Model*.



# Australian critical infrastructure is an attractive target

During FY2023–24, ASD responded to 128 cyber security incidents reported by organisations who self-identified as critical infrastructure. This is a 10% decline compared to FY2022–23. Much of this decline reflects a spike in critical infrastructure reporting from March to April 2023 following website defacement and DDoS incidents linked to hacktivist activity.

The decline may also indicate under-reporting. ASD encourages all Australian critical infrastructure organisations to report anomalous activity early and not wait until malicious cyber activity reaches the threshold for a mandatory report.

## In focus: Australian water and wastewater systems

Globally, water and wastewater organisations provide vital services, including water supply, sewerage and drainage services. To deliver these, the sector relies on a number of increasingly interconnected and internet-connected systems, including information and communications technology (ICT) to bill customers and operational technology (OT) for treatment and distribution.

Malicious cyber actors may target the water sector by exploiting previously unknown vulnerabilities or publicly known common vulnerabilities and exposures, using phishing campaigns to deploy malware targeting ICT and OT systems, compromising passwords, and through supply chain compromises.

Recently reported cyber attacks against the water sector have included ransomware for extortion, access to ICT and OT systems, manipulation of water treatment facilities, and data theft. The effects of these compromises have included an inability to access corporate systems, stolen data, significant remediation costs, and water service disruptions.

In December 2023, the US released an advisory detailing an Iranian Revolutionary Guard Corps-affiliated cyber actor's activity targeting Israeli-developed industrial control systems for water pumps in the US. The US reported that the actor likely gained access by exploiting cyber weaknesses, such as poor password security and unnecessary exposure to the internet.

These cyber security incidents are a timely reminder that practicing good cyber hygiene, including updating default passwords, can help critical infrastructure organisations to guard against malicious cyber activity.

### Case study 3: National Cyber Intel Partnership

Established in September 2023, the National Cyber Intel Partnership (NCIP) is a 2023–2030 *Australian Cyber Security Strategy* initiative, chaired by the National Cyber Security Coordinator, that brings together a group of industry leaders and cyber experts to consider threat intelligence sharing and pilot new threat-blocking capabilities on Australian networks.

In October 2023, the Banking Sector Threat Blocking Working Group was established under the NCIP to focus on phishing as a banking threat and establish the use case through a small pilot program.

The pilot has initially focused on using existing access to threat data and existing threat-blocking capability to build the simplest possible connection to test enhanced information sharing and blocking concepts.

## Operational technology is vulnerable to cyber security incidents

OT comprises systems that detect or cause a direct change to the physical environment through the monitoring or control of devices, processes and events. OT is often used to describe industrial control systems, which include supervisory control and data acquisition (SCADA) systems and distributed control systems. Common OT systems include those used to modify chemical levels in water treatment plants, safety and signalling equipment for rail networks, fire control systems, and electrical switchgear in energy grid substations.

OT systems are a vulnerable target for malicious cyber actors. They are generally designed to run for years or decades to support the delivery of critical goods and services. Where possible, these systems should be segregated from the internet and corporate ICT systems to reduce the risk of cyber attacks. However, in practice, these legacy systems are often connected to ICT networks, can be difficult to patch, and may have vulnerabilities. Furthermore, replacing or updating outdated systems, updating networks, or applying patches can halt the delivery of services, creating operational challenges.

The implementation of OT systems is growing, and ICT and OT networks are increasingly interconnected. This interconnectivity can create greater business efficiencies but can also create cyber vulnerabilities. A cyber security incident affecting ICT can cause service disruptions when OT systems rely on ICT for access, visibility or management of services, even when this is not the intention of the malicious cyber actor. It is important that ICT security is maintained noting the interconnected nature of ICT and OT.

Internationally, malicious cyber activity against OT assets is reportedly on the rise. This trend will likely continue as organisations integrate legacy OT systems with ICT systems in their working environments. It is important that critical infrastructure organisations have a thorough understanding of the threats to OT systems and their business's reliance on these systems. They should continue to segregate these technologies from other networks, such as the corporate network and the internet, where possible.

## Case study 4: NSW energy supplier connection to OT impacted by DDoS

In early 2024, an energy supplier in New South Wales became aware that it had lost remote connectivity with the supervisory control and data acquisition (SCADA) system at two of its sites. SCADA systems are used to gather and process data and apply operational controls. They facilitate the ability of organisations to maintain high-level access to critical systems that may otherwise be difficult to sustain without employees nearby, but also create a vector for malicious cyber actors to attempt access.

The DDoS incident was caused by a brute-force attack targeting a vulnerability in SonicWall Virtual Private Network (VPN) firewall devices. The device – located on the boundary of the energy supplier's OT network – was flooded with thousands of login attempts. The login attempts were unsuccessful due to effective MFA. The device responded by disconnecting all connections, including permitted connections.

Automated alerts of the disconnections began early on a weekend, with all access restored within eight hours. While the ability to remotely monitor SCADA systems was impacted, facilities could still operate using onsite access, meaning there was no interruption to energy supply.

The energy supplier's commercial incident response provider responded to the incident by geoblocking login attempts from outside Australia and returned the firewall device to normal operation after restart. Following this incident, the energy supplier intends to implement Security Assertion Markup Language (SAML) Single Sign-On on their VPN and patch their network devices more frequently.

The energy supplier promptly reported to ASD, which enabled ASD to provide tailored advice on threats to OT systems and support other critical infrastructure providers.

## Case study 5: Targeted briefing activates focused improvements

In April 2024, ASD provided a tailored briefing to an Australian organisation's Chief Executive Officer (CEO) and Chief Information Security Officer (CISO) on specific cyber security threats facing their organisation. Following the briefing, the CEO directed the organisation to mitigate the threats identified by ASD. The organisation undertook both immediate operational actions and advanced longer-term work to improve its cyber security posture. Within four weeks of the briefing, the organisation reallocated over 300 person-hours to address the immediate threats identified by ASD and accelerate planned uplift activities, enabled by support from the organisation's cybersecurity and infrastructure leadership.

The organisation has also increased funding of its security controls improvement program by more than 50% over the next three years to strengthen security controls that mitigate ASD-identified threats. This work is in addition to the organisation's existing cybersecurity investment program. Security and infrastructure teams continue to work together on the design and implementation of the program. The organisation's CISO said 'we really value our long-term partnership with ASD, and the two-way sharing of information and insight. This briefing was particularly helpful in highlighting a specific challenge, and we're glad that ASD was able to make that information available so that we can act on it.'

# Principles of OT cyber security

The principles are designed to assist decision-makers at all levels to give appropriate weight to cyber risks and best secure the systems that keep our nation running. A brief overview of the principles is below. For more guidance, please see ASD's *Principles of OT Cyber Security*, available on [cyber.gov.au](#).



## Principle 1: Safety is paramount – ensure the system is safe.

Safety is critical in physical environments. This includes safety of human life, safety of plant equipment and the environment, and reliability and uptime of the process.

## Principle 2: Knowledge of the business is crucial – know and defend your vital systems.

Knowing the business, how processes work, where connections are and what parts are critical, will help an organisation design and implement the most effective cyber security controls and response capabilities for the resources available. Organisations should be able to identify vital systems and have architecture in place that defends them.



## Principle 3: OT data is extremely valuable and needs to be protected – protect OT data.

For a malicious cyber actor, knowing how a system is set up, on what devices, and with which protocols, is like a treasure map showing how to cause harm. Put processes in place to minimise access to, and distribution of, OT data.



## Principle 4: Segment and segregate OT from other networks – keep the back door shut.

Segment and segregate OT from all other networks, including peers, ICT and the internet. Consider, especially, administrative and management role assignments in OT environments.



## Principle 5: Supply chains must be secure – secure organisational supply chains.

Supply chain security goes beyond software and devices from major vendors. Consider all software, devices and managed service providers in OT.



## Principle 6: People are essential for OT cyber security – people are the first line of defence.

A cyber security incident in OT cannot be identified, resolved, or recovered from without people who have the necessary tools and training. A collaborative team, supported by an appropriate organisational cyber security culture, is a critical element of an organisation's cyber defence.

# Securing critical infrastructure systems

Malicious cyber actors will continue to target Australian critical infrastructure organisations. It is therefore important for these organisations to adopt a stance of ‘when’ not ‘if’ a cyber security incident will occur. To ensure Australian critical infrastructure systems are prepared for, and can quickly recover from, a cyber security incident, ASD recommends that all organisations:

-  understand and map networks. In particular, understand where OT networks connect to partners, vendors, and other systems.
-  implement an event logging system that enables network visibility and the ability to identify cyber security incidents. Further information about event logging can be found in the Resilience chapter.
-  develop and maintain a culture of cyber security awareness, particularly in regard to phishing. A collaborative cyber security culture between ICT and OT teams is essential.
-  follow the *Essential Eight Maturity Model* or an equivalent framework in your ICT environments.
-  maintain an asset registry to manage devices, including OT devices, on all networks. Regularly review the security of these devices. Securely store and protect information about OT systems and assets, and maintain and exercise OT cyber security incident response plans.
-  preference Secure-by-Design and Secure-by-Default products and architectures.
-  review ICT supply chains for vulnerabilities and risks. When engaging a new vendor in the supply chain, review their cyber security practices and policies ahead of implementing their goods and services.
-  review security controls of new software and hardware before purchase and ensure vendor support for future patches and security concerns. Ensure these reviews are extended to industrial plant that may contain embedded systems and controls.
-  limit the use of Remote Desktop Protocols (RDP) and other remote desktop services. If RDP is necessary, apply best practice, including auditing the network for systems using RDP, closing unused RDP ports, and logging RDP login attempts. Further guidance on *Remote Access to Operational Technology Environments* can be found at [cyber.gov.au](http://cyber.gov.au).
-  only connect ICT and OT systems when necessary and ensure these connections are well documented, monitored, and can be segmented before and during a cyber security incident.
-  review the *ASD Principles of OT Cyber Security* and take appropriate action.
-  report anomalous activity, cyber security incidents and vulnerabilities to ASD. Reporting activity that falls below mandatory thresholds, or before a cyber security incident is confirmed, is also encouraged. ASD is not a regulator and timeliness is an important factor when managing a cyber security incident.

## Case study 6: Cyber Operational Resilience Intelligence-led Exercises Framework

The Cyber Operational Resilience Intelligence-led Exercises (CORIE) Framework was developed by the Council of Financial Regulators in 2020 to test and demonstrate the cyber maturity and resilience of institutions within the Australian financial services industry.

Developed to aid in the preparation and execution of industry-wide cyber resilience exercises, the CORIE program is an ongoing series of assessments involving the participation of multiple institutions. CORIE mimics the tactics, techniques, and procedures of real-life adversaries, creating and using tools and techniques that participating institutions may not have planned for or anticipated. These exercises assess the ability of organisations to detect, respond and recover from the operations of a real adversary.

Since its inception, the CORIE program has operated multiple exercises testing financial institutions across banking, superannuation, insurance, financial market infrastructures and critical service providers to the financial services industry. Participation in CORIE is voluntary.

CORIE is producing real-world insights and demonstrates key cyber resilience strengths and weaknesses across the industry. It is also guiding industry to implement best practice cyber resilience testing.

Exercise findings to date have been analysed to identify common strengths and weaknesses, informing relevant Australian regulators of potential systemic weaknesses that may present a risk to the integrity and stability of Australian financial markets. Feedback captured from CORIE participants and from across industry has been resoundingly positive. The Reserve Bank of Australia continues to receive interest from financial institutions to participate in the exercises, demonstrating the positive adoption of CORIE within industry.



# Chapter 3

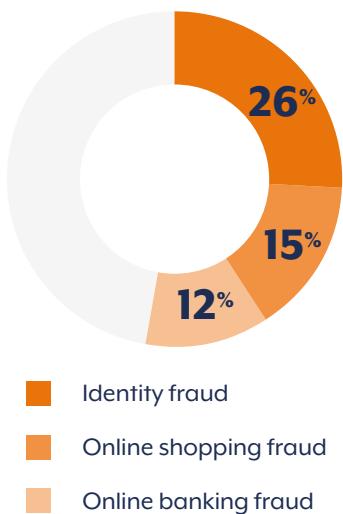


## Cybercrime

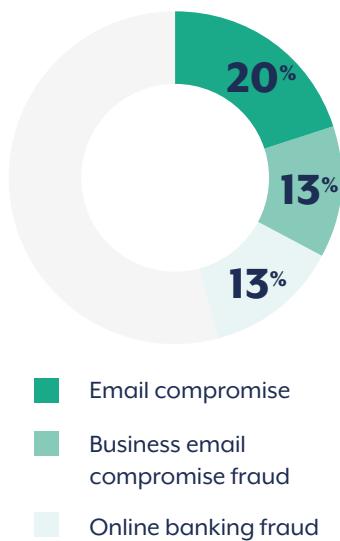
- Ransomware and data theft extortion continue to be pervasive threats, with business email compromise and fraud among the top self-reported cybercrimes for businesses and individuals in Australia during FY2023–24.
- Artificial intelligence continues to shape the cybercrime landscape, with cybercriminals leveraging artificial intelligence tools to conduct increasingly targeted attacks, including social engineering attacks.
- Good cyber security hygiene practices, such as enabling multi-factor authentication for accounts, continues to be one of the best defences against cybercrime.

# Cybercrime in 2023–24

Top cybercrime types for **individuals** reported to law enforcement through **ReportCyber**



Top cybercrime types for **businesses** reported to law enforcement through **ReportCyber**



Top 5 organisations reporting cybercrimes to law enforcement through **ReportCyber**



The difference between email compromise and business email compromise (BEC) fraud is there is a direct financial loss recorded with BEC fraud.

## Average losses

The majority of reports were from **small businesses**, and the impact on business is significant. According to the Australian Bureau of Statistics, in 2022–23,



of businesses had turnover of less than **\$2 million**.

for small business

**\$49,615**    **\$45,965**    **8%**

for medium business

**\$62,870**    **\$97,203**    **-35%**

for large business

**\$63,602**    **\$71,598**    **-11%**

2023–2024

2022–2023

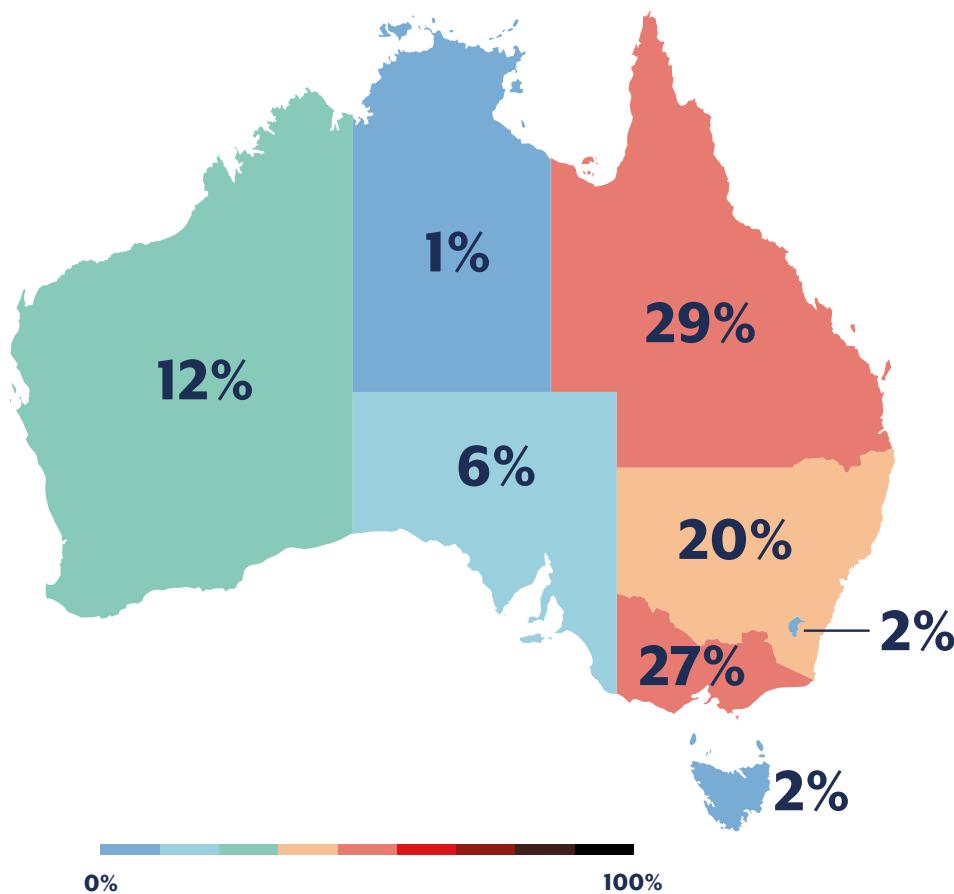
Change

**Table 1:** The average self-reported cost of cybercrime to all businesses decreased by 8% compared to the previous financial year

## Cybercrime reports by state and territory

Australia's more populous states continue to report more cybercrime. Queensland and Victoria report disproportionately higher rates of cybercrime relative to their populations. The highest self-reported financial losses were by victims in New South Wales – around \$86,000 per cybercrime report where a financial loss occurred – followed by those in Victoria, with around \$66,000 per cybercrime report.

The decline in the number of reports can be attributed to the previous financial year's influx of reporting – which arose from high-profile incidents.



**Figure 5:** Breakdown of cybercrime reports by jurisdiction for FY2023-24

*Note: Approximately one per cent of reports came from anonymous reporters and other Australian territories. Data has been extracted from live datasets of cybercrime and cyber security reports reported to ASD. As such, the statistics and conclusions in this report are based on point-in-time analysis and assessment.*

In FY2023–24, the total self-reported BEC losses to ReportCyber were almost \$84 million. There were over 1,400 reports of BEC made to law enforcement through ReportCyber that led to a financial loss. On average, the financial loss from each confirmed BEC incident was over \$55,000. Most confirmed BEC reports came from Queensland (434 reports).

## Case study 7: Medibank and LockBit Cyber sanctions

In January 2024, under the *Autonomous Sanctions Act 2011* the Australian Government sanctioned Russian national Aleksandr Ermakov for his role in the compromise of the Medibank Private network in 2022. This was the first use of the Australian Government's autonomous cyber sanctions framework.

Nearly 10 million personal records were stolen during the cyber security incident against Medibank, including names, dates of birth, Medicare numbers, and sensitive medical information. Some records were published on the dark web.

In May 2024, as part of a separate investigation, the Australian Government imposed Australia's second cyber sanction against Russian national Dmitry Yuryevich Khoroshev, for his senior leadership role in the LockBit ransomware group. LockBit is a prolific cybercriminal ransomware group and works to destabilise and disrupt key sectors for financial gain.

The cyber sanctions imposed by the Australian Government on Ermakov and Khoroshev were targeted financial sanctions and travel bans under the AFP and ASD established Operation AQUILA, together with other Australian government agencies and international partners.

Sanctions are an important part of the Australian Government's toolkit in countering cybercrime. Cyber sanctions impose cost on cybercriminals' ability to operate.

- Cyber sanctions reveal the real-world identities of cybercriminals, undermining their credibility.
- For others in the crime ecosystem, affiliating with a sanctioned cybercriminal could be perceived as higher risk.
- Breaching a cyber sanction can be a serious criminal offence, punishable by up to 10 years imprisonment and/or significant financial penalties.

# Artificial intelligence is changing the cybercrime landscape

The increasing prevalence of artificial intelligence (AI) means that Australia must be responsive to an ever changing cyber threat landscape. Cybercriminals may leverage AI-enhanced social engineering as it is accessible to low-capability actors and can be used to circumvent network defences. For example, AI will allow cybercriminals to undertake more labour intensive activities, such as generating spear phishing content more efficiently and on a larger scale. Cybercriminals may also use AI to create new methods of social engineering attacks, such as imitating a target's voice based on an audio sample.

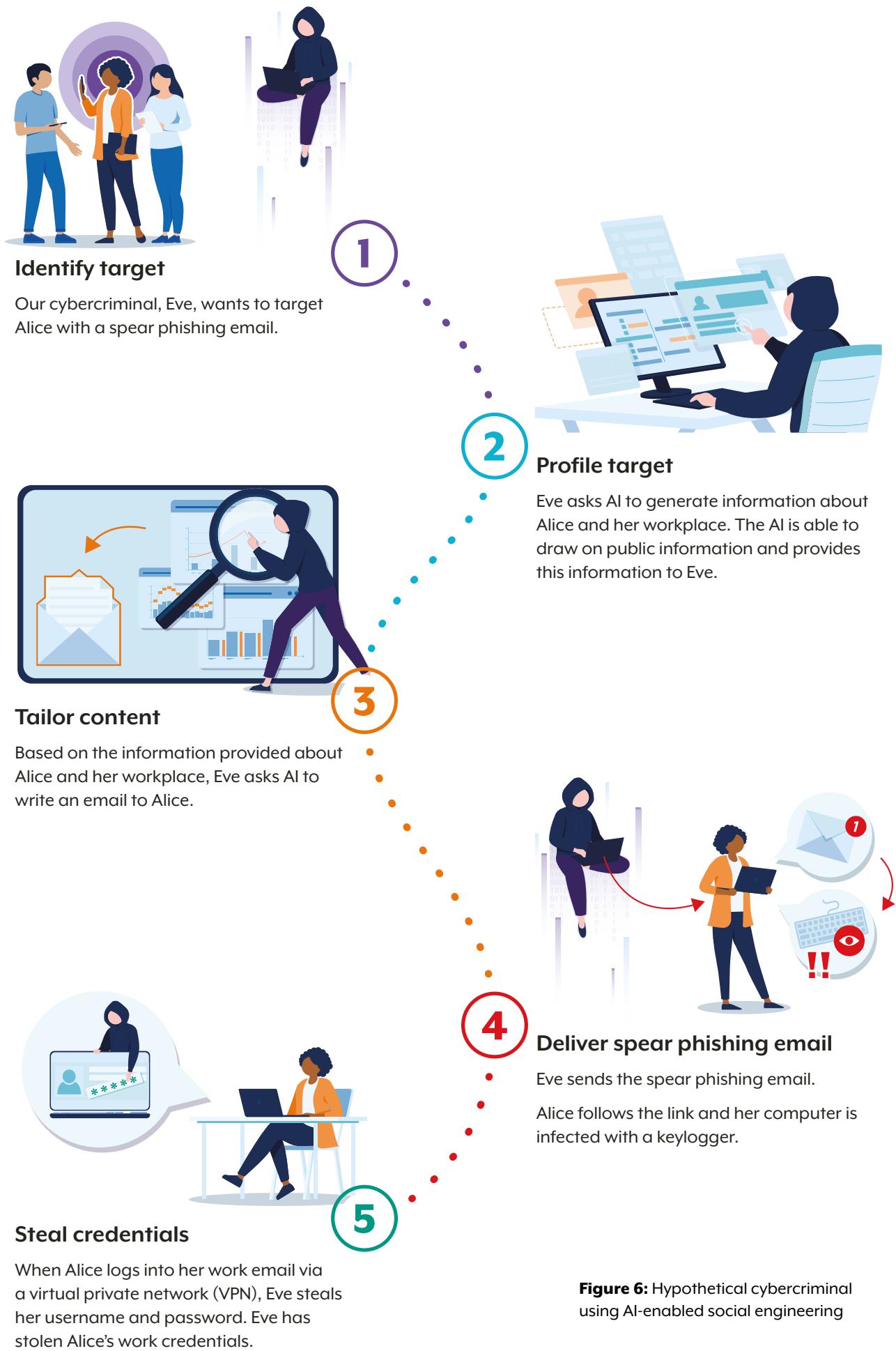
Using AI in social engineering attacks means that cybercriminals can maximise their success rates with little additional effort, increasing the potential for network compromise and the overall threat posed by social engineering.

## Case study 8: Vishing – a video phishing scam

In early 2024, media reported a vishing scam involving a multinational corporation where cybercriminals used AI-generated deepfakes during a video conference call to convince an employee to transfer millions of dollars. The employee initially thought it was a phishing scam, after receiving a message purporting to be the company's UK-based chief financial officer. However, after attending a video conference call and recognising other colleagues in attendance, the employee was reassured the request was legitimate and completed the financial transaction. All attendees at the conference call, except the employee, were deepfake recreations.

Although AI is used by cybercriminals, other applications for AI in cyber security are likely to emerge, including combatting cybercrime. For example, AI can enhance the detection and triage of cyber security incidents and identify malicious emails and phishing campaigns, making them easier to counteract.





**Figure 6:** Hypothetical cybercriminal using AI-enabled social engineering

# Ransomware is persistent and pervasive

Ransomware continues to pose significant operational, financial and reputational risk to Australia.

Ransomware is a type of extortion that uses malware to encrypt data or systems. In FY2023-24, ASD responded to 121 ransomware incidents – accounting for around 11% of all reported incidents. More recently, malicious cyber actors have adjusted their tactics to include stealing sensitive data. Malicious cyber actors then extort payments from victims in return for the recovery of, and ability to regain access to, encrypted data. According to the Australian Institute of Criminology's (AIC) *Cybercrime in Australia 2023* report, 12% of ransomware victims were also extorted for payment to prevent their data being leaked or sold online.

Increasingly, cybercriminals are also exfiltrating data without encrypting victim systems, known as data theft extortion. This data is more attainable for less technically skilled actors, and cybercriminals perceive it is just as lucrative as ransomware given the breadth of Australian organisations that hold sensitive data.

Ransomware attacks are highly destructive, causing significant harm to individuals, organisations, and wider society. For example, businesses may experience reputational damage and financial losses from offline systems and data loss. According to the AIC, small to medium businesses are high-risk targets for ransomware attacks, with small to medium business owners (6.2%) being more likely to be the victim of a ransomware attack compared with employees (3.2%) and individuals who were not small to medium business owners or employees (1.5%).

ASD advises against paying extortion demands. Payment does not guarantee that victims' data is recoverable (even if it is returned) or prevent it from being sold or leaked online. Paying a ransom also encourages the continuation and proliferation of the cybercriminal business model.



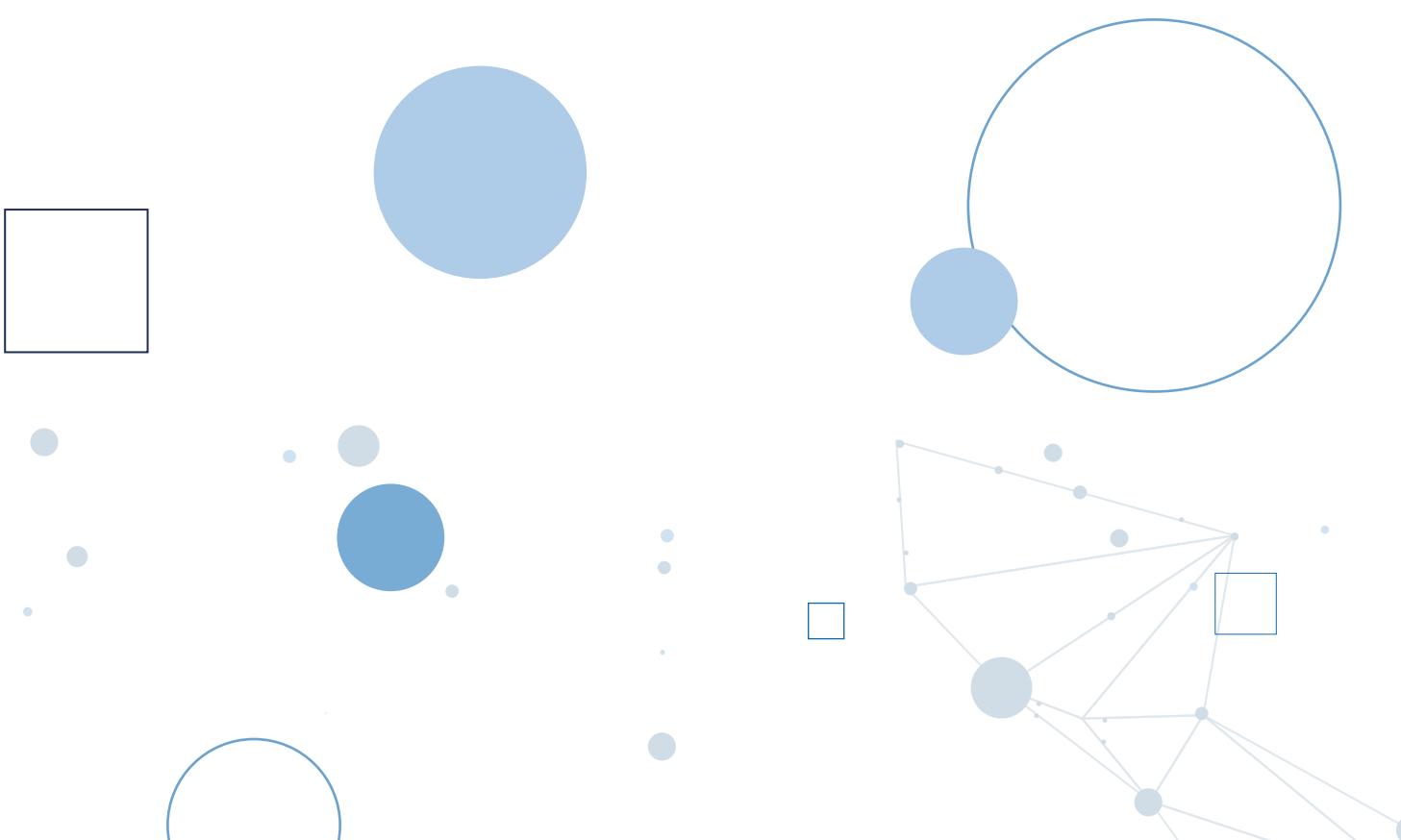
## Countering ransomware groups

### Case study 9: Operation ORCUS

Operation ORCUS is the AFP's ransomware taskforce representing Australia as part of the Europol-led international law enforcement Operation CRONOS. Operation ORCUS is supported by the Joint Standing Operation between the AFP and ASD: Operation AQUILA. Operation AQUILA leverages the complementary powers, capabilities and intelligence of ASD and the AFP to disrupt the most serious cybercrime threats facing Australia.

In December 2023, under Operation ORCUS-PANTHERA, the AFP participated in a global law enforcement operation against the ALPHV/BlackCat ransomware syndicate – seizing criminal infrastructure and websites. The global operation also developed a decryption tool to help victims recover their data and systems. The AFP identified at least 56 Australian businesses and government agencies that had been targeted by the ransomware group. The AFP engaged with those victims to provide decryption keys and restore systems.

In February 2024, under Operation ORCUS-JUNKERS, the AFP participated in a global law enforcement operation that disrupted the world's most prolific ransomware group, LockBit, which has caused billions of dollars in harm across the world – including millions in harm to Australian individuals and businesses. The global operation seized criminal infrastructure, including LockBit's primary platform and 34 servers, more than 200 cryptocurrency accounts, and significant amounts of technical data.



# Common techniques used by cybercriminals

## Credential stuffing – a growing threat for organisations

Credential stuffing – the use of stolen usernames and passwords to access other services and accounts via automated logins – is one of the most common cyber attacks affecting individuals and businesses. When mounting an attack, malicious cyber actors use stolen login credentials across as many websites as possible. Once logged in, they may be able to access victims' accounts without the website or real account holder being alerted. Credential stuffing attacks can cause monetary loss for account holders and identity theft depending on the type of accounts breached and the information stored in them.

Customers often save payment details to websites to speed up transactions, meaning when an account is compromised, a customer's payment details may also be accessed. Victims of credential stuffing are often only made aware of an attack when they are unable to log into their account or when they notice an unauthorised bank transaction and raise it with the business.

According to the AIC's *Cybercrime in Australia 2023* report, 34% of respondents had their financial or personal information exposed in a data breach in the 12 months prior to the survey. Of these, 79% were notified by the company whose data was leaked or by a government or financial agency.

Once a malicious cyber actor's login attempt is successful, they may then engage in other criminal activity, including:

- making fraudulent purchases using victims' stored payment details
- selling personal data and compromised accounts online via the dark web
- using stolen data to commit identify theft and/or to further advance phishing campaigns
- conducting an account takeover, where the threat actor locks the victim out of their account and changes security settings, contact details and other personal details.



In December 2023, a US genetic testing company, 23andMe, notified 6.9 million users that a small percentage of accounts had been compromised due to a credential stuffing attack. Information accessed by the threat actor included ancestry and health-related information. In a separate cyber security incident in 2024, customers of an online Australian retailer had their accounts accessed via credential stuffing, and stored payment details were used to fraudulently purchase goods.

Due to the rise in credential stuffing-related data breaches, individuals and organisations have become increasingly at risk of credential stuffing attacks. The effectiveness of credential stuffing attacks is reliant on passwords being reused across multiple accounts. Any website that requires an online login may be targeted.

A single data breach can place many other accounts and organisations at risk. If a malicious cyber actor accesses a corporate network through a compromised account, such as one belonging to an employee or third-party contractor, they can then move through the network, learning about the system, establishing persistence in the network and stealing data. As access is gained using legitimate credentials, traditional security measures – such as anti-virus software and network intrusion detection systems – often fail to detect the activity.

## Explainer 2: OAIC Notifiable Data Breaches scheme statistics

The Notifiable Data Breaches scheme requires organisations covered by the *Privacy Act 1988* to notify the Office of the Australian Information Commissioner (OAIC) and affected individuals when a data breach involving personal information is likely to result in serious harm.

The OAIC regularly publishes statistical information on data breach notifications it receives to help organisations and the public understand and address privacy risks identified through the scheme.

The OAIC received 1,012 data breach notifications in the FY2023–24, a 13% increase compared to 2022–23. Of the data breaches notified to the OAIC, 41% (or 413 notifications), resulted from cyber security incidents. Of the 413 cyber security incidents:

- 60% involved compromised credentials
- 26% involved ransomware.

Additionally, the OAIC was notified of breaches that resulted from hacking (8%) and malware (4%). Of note, cyber security incidents were the cause of the majority (69%) of large-scale breaches, defined as those affecting 5,000 or more Australians. This included three breaches that affected one million or more Australians.

The risk of outsourcing personal information handling to third parties continues to be a prevalent issue. In the FY2023–24, a high number of large-scale data breaches resulted from a compromise within a supply chain.

The human factor also poses a threat to the strength of an entity's personal information security. Regardless of how secure an entity's systems are, individuals commonly contribute, intentionally or inadvertently, to the occurrence of data breaches.

Further details on the Notifiable Data Breaches scheme are available on the OAIC website.

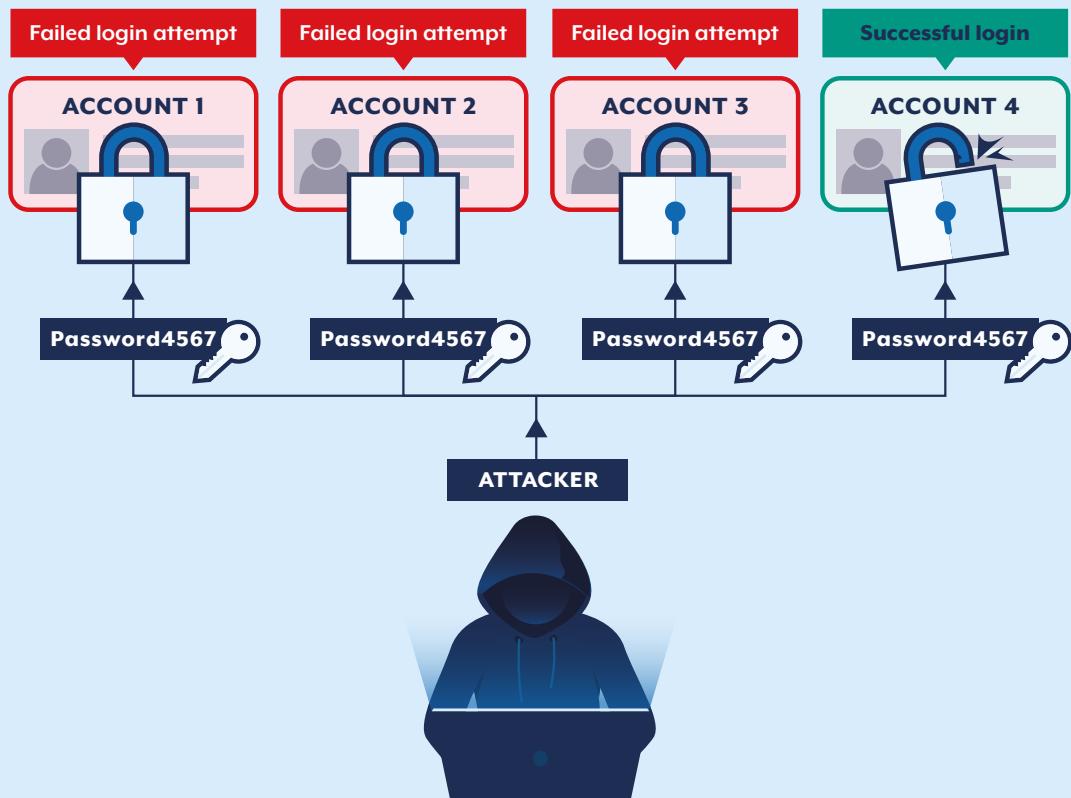
## Password spraying as a high-volume attack tactic

Password spraying is a brute-force attack where malicious cyber actors attempt to access a large number of accounts with commonly used passwords. By trying a single password across several accounts, followed by another single password on the same accounts, malicious cyber actors can circumvent the common cyber security protocol of an account locking after a certain number of failed login attempts within a short period of time.

## Password spraying in practice

When a malicious cyber actor wants to access an organisation's email accounts, they begin by collating a large list of employee email addresses on the dark web, which were obtained through an earlier data breach the company is not yet aware of. Using automated tools, the actor attempts to log into several accounts using one common weak password. The actor repeats this process with different passwords, quickly moving down the list of email addresses. As the actor only attempts a couple of passwords per email address, they avoid detection by the organisation's cyber security system. The actor continues to try different common passwords for each email address until they gain access.

Although simple, password spraying is a highly effective method of attack, able to target hundreds or even thousands of users simultaneously. Because actors can target many users at once, the likelihood of finding at least one or two accounts that use a common, weak password is high. Usually, it only takes access to a single account to provide entry into the broader network, making the organisation vulnerable to further exploitation.



**Figure 7:** Mapped password spraying attack

### Explainer 3: Scams and cyber-related threats – learnings from Scamwatch data

The line between cybercrime (cyber-dependent crimes) and scams (cyber-enabled crime) can blur when scammers use cyber-dependent techniques to commit a scam, such as where malware is used to facilitate a scam. An example of malware-facilitated scams is using adware – which causes splash screens to ‘pop-up’ on victims’ computers. In this example, the victim believes their device has been compromised and is prompted by the pop-up to call a phone number where a scammer impersonates reputable brands, advising of computer security issues. The scammer will then convince the victim to install remote access software on their device to provide full access to the cybercriminals.

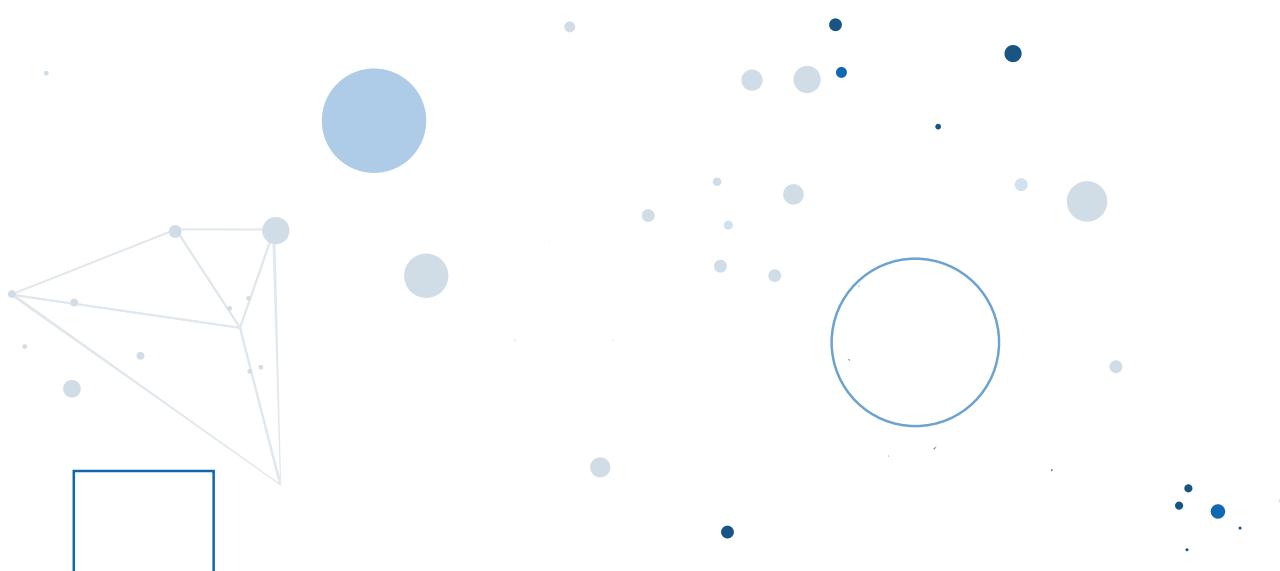
There are five categories where cyber-related threats may be used to facilitate the scams. These are phishing, remote access scams, identity theft (account takeover), hacking, and ransomware and malware scams. It is rare for Scamwatch to receive reports involving true cyber-dependent crimes.

Most scams relate to cyber-enabled crimes, such as phishing. Phishing represents 55% of all losses and 74% of all reports across all five categories in FY2023–24. Together, there were just over 150,000 reports with over \$33 million in losses for these scam types: 1% of these reports mentioned that money was stolen, while 8% mentioned that personal information was stolen.

Credential stuffing and password spraying are known as brute-force attacks. In FY2023–24, 8% of all cyber security incidents responded to by ASD included brute force-related activity. Organisations and individuals with poor cyber security practices, such as shared or repeated passwords, are more vulnerable to a brute-force attack, including by both credential stuffing and password spraying.

ASD recommends using multi-factor authentication (MFA) to defend against the majority of password-related cyber attacks, including credential stuffing and password spraying attacks. MFA requires a combination of two or more of the following factors to access your accounts:

- something you know (for example, a PIN or passphrase)
- something you have (for example, a physical token, authenticator application or email)
- something you are (for example, a fingerprint or facial recognition).



# Quishing – the unseen threat in QR code technology

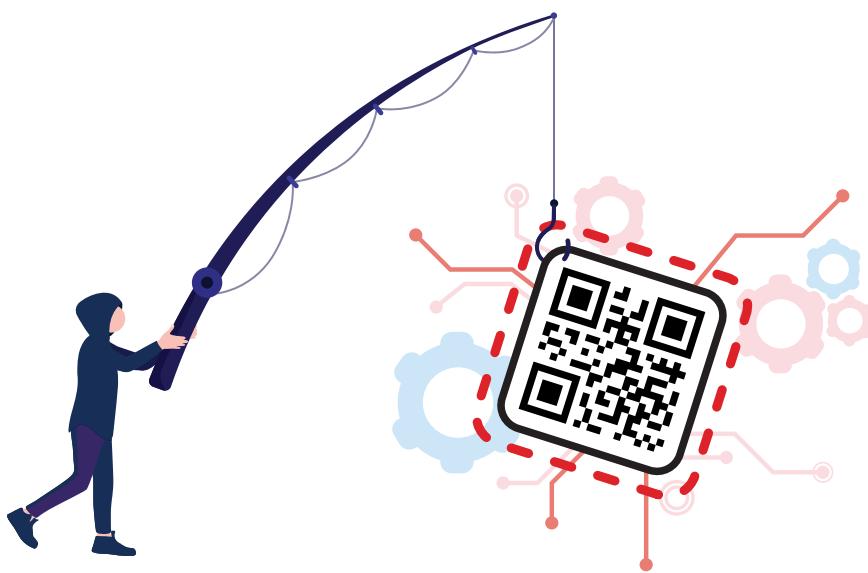
Quick Response (QR) phishing – known as quishing – is a type of phishing attack where cybercriminals use QR codes to trick people into providing personal information or downloading malware onto their smart device. The emergence and rapid expansion of QR codes make a convenient way for users to access information. QR codes are becoming commonplace and used more and more by businesses. For example, scanning QR codes to order from a menu in a local café, or to pay at a parking meter.

People have already placed their trust in this technology. However, the prevalence of QR codes in everyday life presents a potential threat to users, and the effectiveness of quishing attacks is enhanced when cybercriminals exploit this trust. Cybercriminals can embed malicious URLs into QR codes that, when scanned, link to a malicious website or prompt users to download files that can monitor their online activity, steal personal information or gain access to their device. In FY2023–24, ASD responded to 30 quishing-related incidents targeting Australian organisations, demonstrating that social engineering has taken on a new form.

## Case study 10: MFA email scam

In late 2023, the Australian Taxation Office (ATO) released a scam alert, warning of an increase in reports about an email scam impersonating the ATO. The email scam advised clients that due to an ATO security upgrade, they are required to update the MFA on their ATO account. The scam email included a QR code that linked to a fake myGov login page, designed to steal clients' myGov account details.

Once a scammer has access to an individual's myGov account, they may be able to make fraudulent lodgements and change bank details so that any payments are redirected to a scammer's account.



# Defending against and deterring cybercrime

Everyone must play a role in enhancing cyber security and reducing the risk of cybercrime. We encourage all Australians to:

- turn on MFA for accounts
- use long, unique passphrases for each account, especially if MFA is not available
- check automatic updates are on and install new updates as soon as possible
- back up important files and device settings regularly
- be alert for phishing messages and scams
- sign up for ASD's free Alert Service
- report cybercrime, cyber security incidents and vulnerabilities through ReportCyber at [cyber.gov.au](http://cyber.gov.au).

ASD also has several resources available to individuals, businesses and government to help improve cyber security, including:

- *Personal Security Guides*
- *Small Business Cyber Security Guide*
- *Practical Cyber Security Tips for Business Leaders*.



## Case study 11: ASD assists AISNSW in discovery of malware

To an onlooker, a not-for-profit organisation in the education sector would seem an unlikely target for cybercrime. However, malicious cyber actors frequently target the education sector, as the Association of Independent Schools of NSW (AISNSW) found out when they were alerted to malware lurking on their system.

AISNSW first became aware of the malware in November 2023 when ASD sent them a notification advising that Gootloader malware had been detected on one of their devices. Gootloader is an ‘Initial Access as a Service’ tool used to distribute other forms of malware.

The malware infected the system when an employee searched online for an Australian education sector enterprise agreement and clicked on a malicious sponsored link – a technique known as search engine optimisation (SEO) poisoning. This sent the employee to a honeypot website designed to look like an online forum. The employee downloaded a ZIP file purporting to be a copy of the enterprise agreement posted by a forum user. This executed the Gootloader payload.

The malicious cyber actor had persistent access to the network for three days. While the actor did not conduct command-and-control activities on the network, they may have been positioned to on-sell the access to another cybercriminal to use for ransomware or data theft.

Within two hours of receiving the notification from ASD, AISNSW’s ICT team had isolated the infected device and enacted controls to remediate the issue. Subsequently, the device was reimaged. In the following days, AISNSW worked with both ASD and the AFP, providing indicators of compromise (IOCs) to help prevent future compromises of other organisations.

It was through AISNSW’s membership of ASD’s Cyber Security Partnership Program that they were able to get timely advice directed to the right people within their organisation, expediting remediation. AISNSW has been a member of the ASD’s Cyber Security Partnership Program since March 2023. Since the compromise, AISNSW has been encouraging their contacts within the education sector to join the Partnership Program.

‘The ASD’s Cyber Security Partnership Program has proven invaluable to us in many ways, but in this instance it literally saved us from a potentially significant cyber incident,’ said Marcus Claxon, Manager: Cyber Security and Infrastructure Advisory Services at AISNSW.

‘It has also demonstrated the benefits of government and organisations working together in our cyber defence efforts.’

## Case study 12: Operation ZINGER

The AFP's Operation ZINGER is an investigation into Australian alleged offenders purchasing and using compromised Australian devices. Operation ZINGER is the AFP's parallel investigation, with US Federal Bureau of Investigation's 'Operation Cookie Monster', into the illicit online marketplace named Genesis Market.

Genesis Market was an invitation-only marketplace that sold login details, web-browsing cookies and other sensitive information stolen from compromised devices and computers around the world. Buyers could obtain access to banking and personal information – details that could be used to access government services.

A globally coordinated operation occurred in April 2023, involving the takedown of Genesis Market, with more than 100 people arrested as a result of more than 300 police actions across 17 countries.

In Australia, the AFP-led Joint Policing Cybercrime Coordination Centre coordinated the overt phase involving 27 search warrants across (and in conjunction with) multiple states and territories. The operation disrupted individuals alleged to be buying stolen personal information via Genesis Market in order to commit various fraud or cybercrime offences, including against financial institutions and government agencies. The AFP identified more than 36,000 compromised Australian devices available for sale on Genesis Market, part of approximately two million sets of credentials, including those containing details from myGov and Australian financial institutions.

Along with Australia, 17 other countries were involved in this operation: the US, the Netherlands, Spain, France, Finland, Germany, Italy, Poland, Romania, Sweden, Denmark, Canada, Switzerland, the UK, Iceland, New Zealand and Estonia.

To date, 12 alleged offenders have been arrested and charged in Australia with cybercrime offences.



**AFP**



# Chapter 4



## Hacktivism

- Rising global tensions have resulted in an increase in hacktivist activity around the world, adding further complexity to the cyber-threat landscape.
- Hacktivists tend to be less capable and have fewer resources than other malicious cyber actors. They often employ publicly available tools to disrupt services and further their cause.

The term hacktivism is often used to describe a person or group who uses malicious cyber activity to further social or political causes, rather than for financial gain. Hacktivists – also known as issue-motivated groups – use technical hacking skills to fight for a cause, a political view or to expose a perceived injustice.

The three main motivators of hacktivism are:

- patriotic: hackers act in support of the perceived goals of a state, often against targets they view as opposing the state's interests. Patriotic hacking is often triggered by territorial disputes.
- issues motivated: hackers act to expose perceived social injustices, corruption, or political repression.
- ideologically motivated: hackers seek to promote political or religious beliefs or agendas.

Hacktivist groups conduct malicious cyber activity to affect business operations and embarrass, threaten or intimidate their victims – including governments, businesses and individuals.

Examples of hacktivist activity include:

- Denial of Service attacks
- website defacements
- hijacking of official social media accounts
- public disclosure, or doxxing, of sensitive or personally identifiable information.

Hacktivists are typically less capable, organised and resourced than other types of malicious cyber actors, such as state-sponsored cyber actors. However, hacktivists can leverage publicly available tools and services to gain new capabilities and improve their ability to degrade or disrupt services for their cause. This can result in real-life consequences.

Hacktivist activity has significantly increased in recent years, adding to an already complex cyber threat-landscape. This is partly due to changes in the geopolitical landscape, including conflicts, and the broad reliance on the internet, social media and other types of digital communication.

### Case study 13: Sanctioning members of the Cyber Army of Russia Reborn

In July 2024, the US sanctioned Yuliya Vladimirovna Pankratova and Denis Olegovich Degtyarenko, two members of the Russian government-aligned hacktivist group Cyber Army of Russia Reborn (CARR). Pankratova and Degtyarenko were sanctioned for their roles in cyber operations against US critical infrastructure.

Since 2022, CARR has conducted low impact, unsophisticated Distributed Denial of Service (DDoS) attacks in Ukraine and against governments and companies located in countries that have supported Ukraine. In late 2023, CARR claimed responsibility for attacks on the industrial control systems of several US and European critical infrastructure targets, including water supply and energy facilities. Most recently, in January 2024, CARR claimed responsibility for an attack on water storage tanks in Texas, causing the loss of tens of thousands of litres of water. However, despite CARR briefly gaining control of these industrial control systems, significant damage to victims has been limited due to CARR's lack of technical sophistication.

# Chapter 5



## Resilience

- Cyber resilience is about preventing and quickly recovering from a cyber security incident. For larger organisations, this includes entity-wide cyber risk management that considers how to manage information and communications technology supply chain risks and safely use new technologies.
- ASD encourages organisations to implement the *Essential Eight Maturity Model* and apply the *Information Security Manual* cyber security framework to protect their systems and data from cyber threats. Practices should include replacing or applying appropriate protections to legacy systems, and ensuring new products are Secure-by-Design.
- Everyone should practise good cyber hygiene: enable phishing-resistant multi-factor authentication, make sure passwords and passphrases are secure, and keep your devices up to date.

## Edge devices

An edge device is any piece of hardware that controls data flow at the boundary between two networks – including routers, virtual private network (VPN) products and firewalls. Malicious cyber actors target edge devices because they are often connected to both the internet and an internal network. Additionally, some devices are exposed to easily exploited vulnerabilities, providing a convenient pivot point. By compromising edge devices, malicious cyber actors can access data traversing the device and may be able to move laterally into a victim's network, stealing more valuable data from internal systems.

## Exploitation of SOHO routers poses a significant risk to individuals and small businesses

Small-office/Home-office (SOHO) routers are the edge devices that connect most Australian homes and small offices to the internet. They include the default routers that internet service providers typically supply to new customers. Approximately 8.3 million Australian residential internet connections rely on a SOHO router, and it is very likely that a considerable number of these routers are exposed and vulnerable to malicious cyber actors.

Australian SOHO routers are an attractive target for malicious cyber actors. Publicly available search engines can be used to find information about SOHO routers, including their IP addresses and software/firmware. SOHO devices are of high interest to malicious cyber actors because they can gain valuable information with a low barrier for entry.

The exploitation of SOHO routers poses a significant cyber security risk. A compromised router can be used for multiple purposes, including gaining access to the victim's network with the aim of stealing data. It could also be used in further attacks through a botnet – a collection of devices infected by malware and remotely controlled by an actor, without the owner's knowledge. A malicious cyber actor uses a botnet to launch cyber attacks, leveraging the infected device's hardware and processing power.

To mitigate these risks and keep networks safe, it is important to secure SOHO routers:

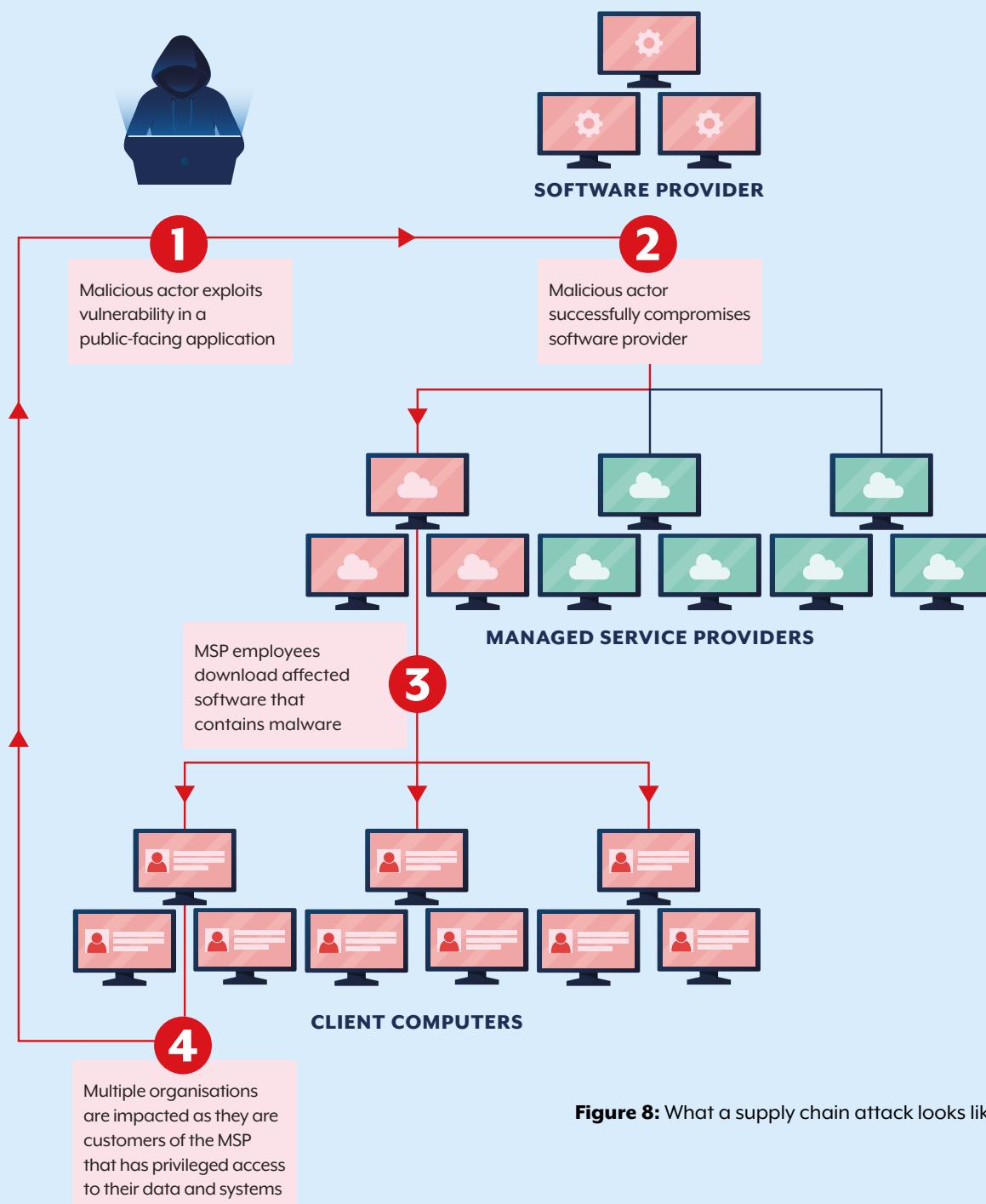
- keep your router up to date and enable automatic updates, where possible
- change the default Wi-Fi network name and password you use to access your router's settings
- change your router's default username and password.

Further advice can be found on the *Secure your wi-fi and router* page on [cyber.gov.au](http://cyber.gov.au).

# ICT Supply Chains

An organisation's cyber security posture is only as strong as its weakest link. All organisations have some component of their information and communications technology (ICT) outsourced to a third party, such as hardware supply, web and data hosting and Software as a Service or other enterprise resource planning tools. Therefore, organisations must assess and monitor all software and services they procure and consume and consider the cyber security of their providers.

When an organisation grants a supplier privileged access to their systems, they are vulnerable if the supplier becomes compromised. If a supplier is compromised, it can result in the compromise of multiple customer systems. By compromising a supplier, a malicious cyber actor can better obfuscate their activities – providing advantage over direct targeting.



**Figure 8:** What a supply chain attack looks like

Cyber supply chain incidents have resulted in millions of Australians having their information stolen and leaked on the dark web. Other business impacts reported to ASD include:

- shipping delays to medical products
- outages for sensitive monitoring systems
- release of commercial-in-confidence data.

In FY2023–24, ASD responded to 107 cyber supply chain incidents. Cyber supply chain-related incidents comprised 9% of all cyber security incidents responded to by ASD. These incidents commonly involved compromised assets, networks and/or infrastructure (26%), compromised accounts and/or credentials (24%) or data breaches (20%).

It is essential that organisations undertake due diligence on a supplier's products and cyber security practices before and while engaging suppliers. Further advice on supply chain risk assessment and management can be found at [cyber.gov.au](https://cyber.gov.au), including:

- *The Information Security Manual (ISM)*
- *Choosing Secure and Verifiable Technologies*
- *Cyber Supply Chain Risk Management*
- *Exercise in a Box*.

## **Case study 14: NDIS disability support provider reports Citrix gateway compromise**

On 21 November 2023, a disability support provider reported to ASD that their network had been compromised using a vulnerability in their Citrix NetScaler Gateway. The organisation has numerous locations across Western Australia, supporting thousands of Australian individuals living with disabilities. The health sector is a valuable target for malicious cyber activity because of its highly sensitive personal data holdings, the criticality of its services, and the public trust in health sector organisations.

The vulnerability, CVE-2023-4966, is known as Citrix Bleed. It has affected multiple Australian organisations. The vulnerability allows a malicious cyber actor to exploit a vulnerability and bypass multi-factor authentication (MFA) to obtain sensitive information and conduct session hijacking.

The reporting organisation's ICT team identified that the unauthorised Citrix session was from a non-Australian IP address and within 75 minutes had geo-blocked certain overseas IP ranges on their firewall to prevent further attacks. While Citrix allows multiple concurrent sessions per user by default, the organisation's ICT administrator had discerningly set Citrix to allow only one session per user. This restricted the actor's connectivity to the network, and no other fraudulent sessions or users were identified in the logs.

The organisation was proactive in disabling all access to Citrix servers within three hours of the unauthorised activity and resetting all potentially vulnerable passwords. No privilege escalation was identified, and MFA was already enforced on most applications. There was minimal business impact with only two affected users.

This cyber security incident demonstrates the importance of patching applications and enforcing MFA. Further details about the Citrix Bleed vulnerability and mitigation guidance can be found in the advisory *Citrix Products NetScaler ADC and NetScaler Gateway Vulnerabilities*.

## Secure-by-Design

Technology manufacturers and consumers must ensure the security of their digital products and services by adopting ‘Secure-by-Design’ culture and practices.

Secure-by-Design is a proactive, security-focused approach to the design, development and deployment of digital products and services that necessitates the strategic alignment of an organisation’s cyber security goals. The overarching goal of Secure-by-Design is to protect consumer privacy and data by designing, building and delivering products with fewer vulnerabilities, and maintaining security throughout the product’s lifecycle.

Over FY2023–24, ASD embarked on a comprehensive program of work, as part of a wider international effort, to promote and uplift industry and government’s ability to implement Secure-by-Design. In September 2023, ASD released the Secure-by-Design Foundations.

The Foundations have been created to promote a common understanding of the responsibilities of technology manufacturers and consumers to develop, deploy, and sustain secure digital products and services. Under each foundation, key risks, focus areas and benefits have been identified separately, for both technology manufacturers and consumers. This approach allows manufacturers and consumers to work together to ensure products are developed and used with security considered throughout its entire lifecycle.

Since releasing the Foundations, ASD has co-developed and co-sealed several Secure-by-Design publications with international partners, including:

- *Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and Default*
- *The Case for Memory Safe Roadmaps*
- *Choosing Secure and Verifiable Technologies.*

## Event logging

Event logging is an important part of network visibility and cyber security. Event logging refers to the automatic production of time-stamped documentation that details events relevant to a particular system. Many applications record errors and events in proprietary error logs, each with their own format and user interface. An effective event logging solution provides a centralised facility for network defenders to search and monitor important events. Event logging supports the continued delivery of critical systems and improves the security and resilience of systems by enabling network visibility. An effective logging solution aims to:

- identify cyber security incidents, such as malicious cyber actors employing living off the land (LOTL) techniques or lateral movement, post-compromise
- support incident response by revealing the scope and extent of a compromise
- monitor account compliance with organisational policies
- reduce alert noise, saving on costs associated with storage and query time
- enable defenders to make agile and informed decisions based on actionable alerts (exclusive of false positives).

ASD recommends that organisations implement a log collection strategy focused on capturing high-quality events to enable effective threat detection. For more information on best practice, organisations should review the *Best Practices for Event Logging and Threat Detection* on [cyber.gov.au](http://cyber.gov.au).

# Cloud computing and the shared responsibility model

Cloud computing – a delivery model for information and communications technology services – is a model that enables network access to a shared pool of computing resources, such as data storage, servers, software applications and services.

Cloud security is a shared responsibility between the cloud service provider, the cloud consumer and any other third parties involved in providing a complete cloud solution. Consumers need to understand their responsibilities, as well as the responsibilities of the other parties. Despite the shared responsibility model, it is important to note that the customer organisation will always be responsible for:

- ensuring that cloud computing services meet the organisation's security needs
- securely configuring cloud computing services used by the organisation
- deciding which data the organisation stores in cloud computing services.

Broadly, there are three cloud computing service models:

- **Infrastructure as a Service** (IaaS): The vendor provides physical computer hardware, including central processing unit (CPU) processing, memory, data storage and network connectivity
- **Platform as a Service** (PaaS): The vendor provides IaaS plus operating systems and server applications, such as web servers
- **Software as a Service** (SaaS): The vendor uses their cloud infrastructure and platforms to provide customers with software applications, such as email (for example, Microsoft 365).

## Explainer 4: ASD's Blueprint for Secure Cloud

In late 2023, ASD published ASD's *Blueprint for Secure Cloud* (the Blueprint), a refreshed version of the Digital Transformation Agency's *Protected Utility Blueprint*. The Blueprint is an online tool, published as both a website and GitHub repository, which supports the design, configuration and deployment of collaborative and secure cloud and hybrid workspaces, with a current focus on Microsoft 365. It provides best practice guidance and templates covering risk management, architecture, and standard operating procedures developed as per the controls in ASD's *Information Security Manual* (ISM).

ASD published Microsoft 365 Desired State Configuration (M365DSC) files as part of the Blueprint in May 2024. M365DSC supports organisations to configure new Microsoft 365 tenants by partially automating deployment of the Blueprint's recommended configuration.

The guidance and advice in the Blueprint are informed by the experience gained by ASD in responding to cyber security incidents, performing vulnerability assessments and penetration testing Australian government organisations. ASD will continue to use cyber threat intelligence and feedback from partners across government and industry, to ensure the Blueprint remains contemporary, fit for purpose and actionable. ASD's *Blueprint for Secure Cloud* is an open source project and input is welcome from all Australians. To get involved, visit [blueprint.asd.gov.au](https://blueprint.asd.gov.au).

# Securing artificial intelligence

Artificial intelligence (AI) systems are among the fastest growing applications globally. AI drives internet searching, satellite navigation, and recommendation systems. AI is also increasingly used to handle activities traditionally undertaken by humans, such as sorting large data sets, automating routine tasks, undertaking creative endeavours and augmenting business activities. For example, customer engagement, logistics, medical diagnoses, and cyber security. AI is being incorporated into consumer products that are used in daily life.

While AI has the potential to increase efficiency and lower costs, its use can also, intentionally or inadvertently, cause harm. To take advantage of the benefits of AI securely, individuals and organisations should take some time to understand what risks apply to them and how those risks can be mitigated.

As with any software program, AI systems should be patched and kept up to date to avoid exposure to vulnerabilities. Some common AI-specific risks are outlined below.

- **Data poisoning:** An AI model is built by training it on a large amount of data. As the quality of training data affects the performance of the AI model, a malicious cyber actor that alters this training data could influence the AI to make poor or incorrect decisions.
- **Adversarial inputs:** Once an AI system is in operation, malicious cyber actors may be able to provide it with specially crafted inputs or prompts to force it to make a mistake, such as by generating sensitive or harmful content.
- **Privacy concerns:** Data collected from individuals is often anonymised to protect their privacy. When anonymised correctly, it should require a substantial effort to re-identify an individual. However, with the emergence of AI, there are concerns that malicious cyber actors may be able to re-identify individuals in large sets of anonymised data by leveraging AI.
- **Hallucination:** AI may make incorrect predictions or generate false positives or false negatives. AI has provided false references that do not exist.



# Secure use of AI

There are steps that individuals and organisations can take to engage with AI securely. The questions below can help identify AI risks and mitigations:

## Individuals

- Does this AI system have a good reputation?
- Do I need to share this information with the AI system?
- How will the AI system use my information? What does its privacy policy say?
- What can I do to ensure the output of the AI system is accurate and appropriate for use?

In addition to releasing *An Introduction to Artificial Intelligence*, ASD also co-developed and co-sealed several AI publications with international partners, including:

- *Engaging with Artificial Intelligence*
- *Deploying AI Systems Securely: Best Practices for Deploying Secure and Resilient AI Systems.*

## Organisations

- Does our organisation understand the AI system, including the risks it poses?
- Is the AI system Secure-by-Design?
- Have we identified cyber supply chain risks associated with the AI system?
- How will the AI system affect our organisation's privacy and data protection obligations?
- Who is accountable for oversight and/or if something goes wrong with the AI system?
- What access does the AI system have to our organisational intellectual property and does it use our material to answer other organisations' questions?
- What level of trust do we place in AI systems and answers provided?

# Phishing-resistant multi-factor authentication

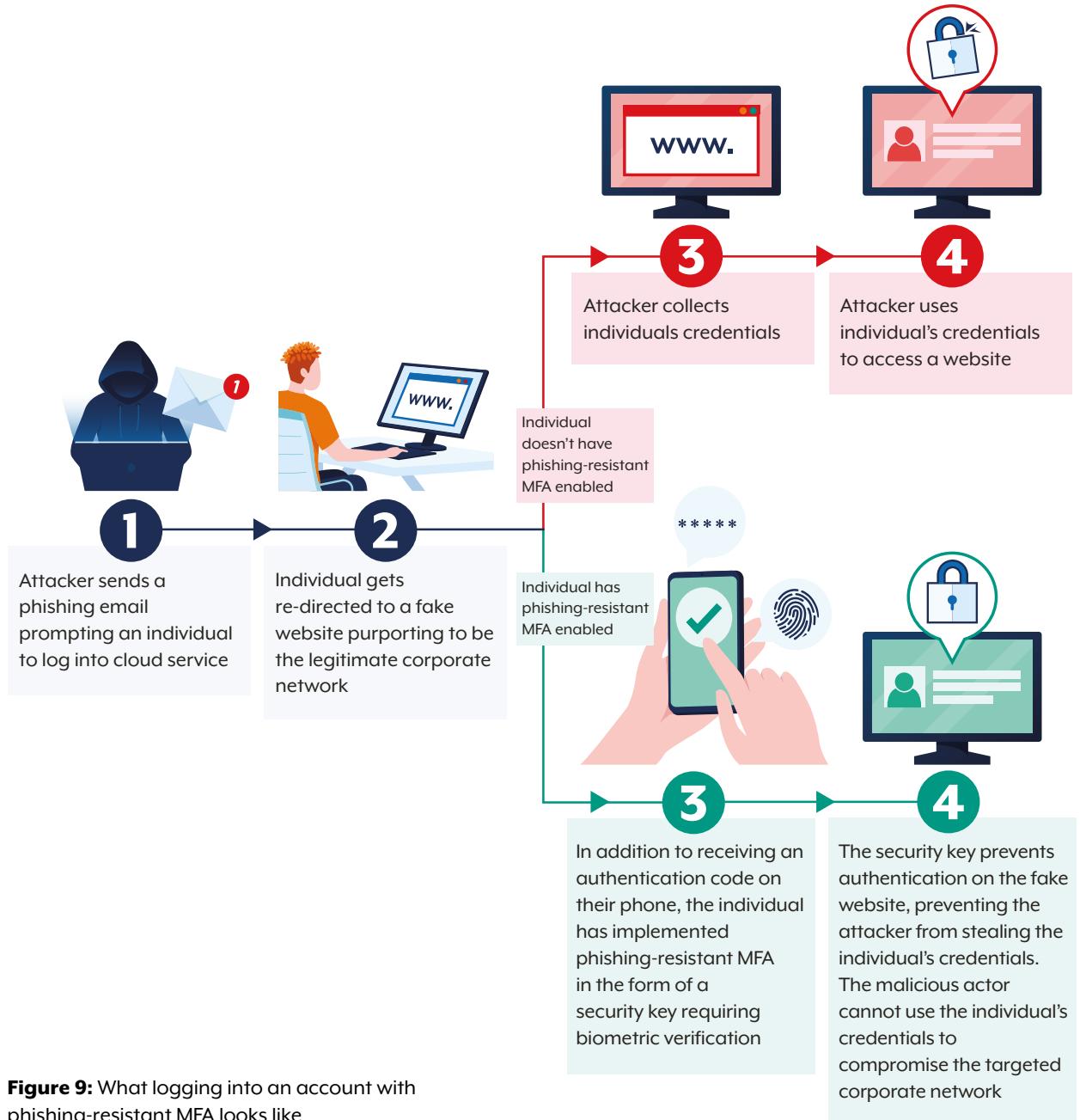
Malicious cyber actors often target remote access systems, email systems, and file servers to gain access to sensitive data. To do this, they use phishing – often in the form of an email – to take advantage of, and trick, unsuspecting victims. Phishing correspondence will often ask a victim to update or enter personal information or login details via a malicious link or attachment. This can enable a malicious cyber actor to take over the victim's account, steal their identity and potentially initiate secondary exploitation, such as ransomware attacks or data breaches.

Non-phishing-resistant MFA, such as passwords, SMS, other one-time passwords, security questions or push notifications, do not protect individuals and are especially susceptible to phishing. A malicious cyber actor may trick a victim, on a fake website that purports to be the legitimate corporate network, into using their password and a unique MFA code either texted to a mobile device or generated in a mobile app. The malicious cyber actor can then use the victim's credentials to gain access to the victim's real account via the real website.

Phishing-resistant MFA can help to mitigate phishing activity. Authentication requires a private key that is secured in a hardware device, instead of software alternatives. Secure authentication not only requires that each individual provides proof of their identity, but also of intent through deliberate action. Currently, there are two authentication methods that satisfy the requirements for phishing-resistant authentication: Personal Identity Verification smart cards, and physical and digital security keys that are supported by FIDO2/WebAuthn standards. These standards support authentication to online services.

While organisations and individuals are encouraged to adopt phishing-resistant MFA to keep up with the advanced tradecraft used by malicious cyber actors, it is worth noting that if phishing-resistant MFA is not available, individuals should still implement MFA as it provides better protection than just passwords alone.





**Figure 9:** What logging into an account with phishing-resistant MFA looks like

Implementing phishing-resistant MFA adds an extra layer of security that makes it harder for malicious cyber actors to gain access to confidential data.

# The Essential Eight

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

The *Essential Eight Maturity Model* supports the implementation of the Essential Eight. It is based on ASD's experience in producing cyber threat intelligence, responding to cyber security incidents, conducting penetration testing and assisting organisations to implement the Essential Eight.

The mitigation strategies that constitute the Essential Eight are:



## 1. patch applications



## 2. patch operating systems



## 3. multi-factor authentication



## 4. restrict administrative privileges



## 5. application control



## 6. restrict Microsoft Office macros



## 7. user application hardening



## 8. regular backups

Assessments against the Essential Eight should be conducted using the *Essential Eight Assessment Process Guide*.

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. ASD has also developed an Essential Eight assessment course in partnership with TAFEcyber to support the security knowledge and assessment skills of cyber security professionals across Australia.

Further information on the *Essential Eight Maturity Model* and its implementation is available in the *Essential Eight Maturity Model FAQ* publication at [cyber.gov.au](https://cyber.gov.au).

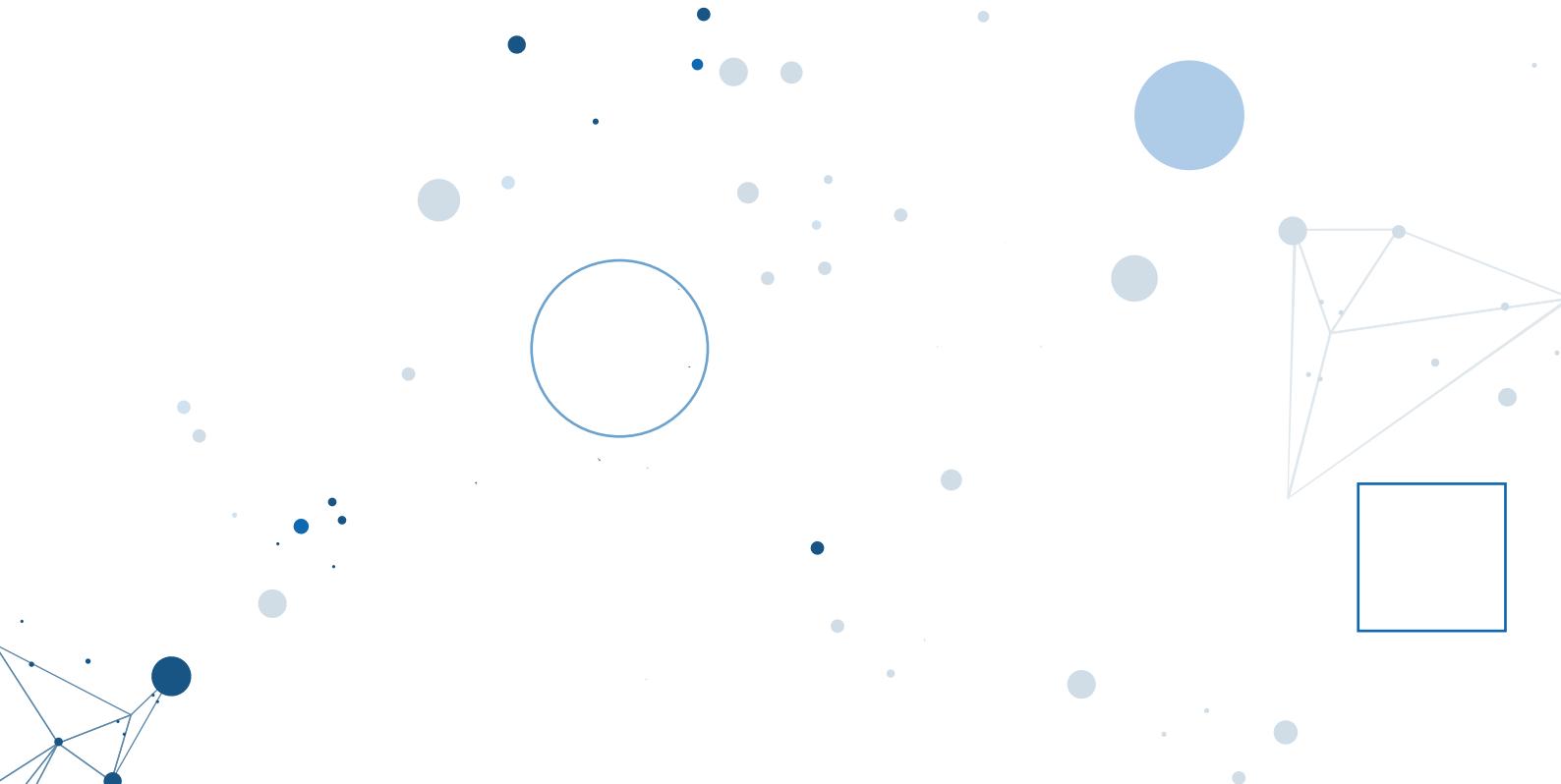
# Information Security Manual

ASD's *Information Security Manual* (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 information technology managers.

The ISM is updated regularly and the latest version, released in September 2024, can be found on [cyber.gov.au](https://cyber.gov.au).

## Explainer 5: Essential Eight Maturity Model versus Information Security Manual

- Organisations should consider their Essential Eight Maturity Model and ISM requirements independently. For example, an organisation contractually required to implement Maturity Level Two from the Essential Eight Maturity Model should not assume that controls within the ISM that are mapped to Maturity Level Three are out of scope when building and deploying a system.
- The ISM also provides *Open Security Controls Assessment Language baselines for the Essential Eight Maturity Model* that organisations can use to track implementation of the Essential Eight Maturity Model within their governance, reporting and compliance tools.
- A map between the Essential Eight Maturity Model and ISM is provided within the *Essential Eight Maturity Model and ISM Mapping* publication.



# Chapter 6



## ASD programs

- Collaborative partnerships between and across the public and private sectors are an integral part of building Australia's cyber resilience. To foster these relationships, ASD offers a range of programs for both industry and government.
- The Partnership Programs bring together industry and government to share and overcome cyber security challenges and build Australia's collective cyber resilience.
- Report cyber crimes, cyber security incidents and vulnerabilities to [cyber.gov.au/report](http://cyber.gov.au/report) or 1300 CYBER1 (1300 292 371).

# Engaging with ASD

The speed with which cyber threats spread and evolve means that no single person or organisation can effectively defend against all threats in isolation. Cooperation on a national and international scale is one of Australia's greatest advantages against malicious cyber activity.

It is vital that cybercrime, cyber security incidents and vulnerabilities are reported to ASD. Reporting helps build a national cyber threat intelligence picture and helps ASD to provide timely technical advice and assistance.

There are many ways in which Australian organisations can engage with ASD to improve their own cyber security and help boost Australia's cyber defences.

**The ASD's Cyber Security Partnership Program** enables eligible Australian organisations to engage with ASD and industry and government partners, drawing on collective understanding, experience, skills and capability to lift cyber resilience across the Australian economy. ASD's Cyber Security Partnership Program is a national program, delivered through ASD's state offices located around Australia.

An ASD's Network Partnership is available to organisations with responsibility for the security of a network or networks (either their own or on behalf of customers) as well as academic, research and not-for-profit institutions with an active interest and expertise in cyber security. An ASD's Business Partnership is available to those with a valid Australian Business Number (ABN). Individuals and families can sign up to the ASD's Home Partner Program.

Through the Partnership Programs, Australian organisations can draw on the collective understanding, experience and capability of the community to lift Australia's cyber resilience. ASD's Network Partners bring their insights and technical expertise to the community to collaborate on shared threats and opportunities.

**The Critical Infrastructure Uplift Program** (CI-UP) assists Australian critical infrastructure organisations to improve their resilience against cyber attacks, with a focus on critical infrastructure assets and OT environments. As a voluntary, intelligence-driven program, CI-UP focuses on improving the cyber security of critical infrastructure in a range of areas, including:

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



**The Cyber Uplift Remediation Program** (CURP), formally known as ACSC's Cyber Security Uplift Services for Government (ACSUSG), enables priority Australian government organisations to improve their cyber security posture. The objective of CURP is to uplift Essential Eight maturity, improve cyber security posture, and remediate other cyber security vulnerabilities through the provision of skilled technical specialists and working in partnership with prioritised government organisations. The CURP implements security controls and offers further recommendations aligned with the findings of ASD, as well as advice and services provided through complementary services.

### Case study 15: CURP – helping to uplift Australian government organisations

In 2022, an Australian government organisation underwent a cyber security assessment by the Cyber Maturity Measurement Program, which revealed an Essential Eight maturity score of zero for all mitigation strategies. This was indicative of weaknesses in their security posture that could be exploited by malicious actors using basic tactics, techniques, and procedures.

The organisation was constrained by the available resources. However, ASD worked with the organisation to successfully implement Essential Eight Maturity Level One and Two mitigation strategies over 18 months.

**The Cyber Maturity Measurement Program** (CMMP) engages with prioritised federal, state and territory government organisations to assess their maturity with the Essential Eight Mitigation Strategies and their broader cyber security posture.

The CMMP favours coverage over evasion and attempts to identify as many vulnerabilities, misconfigurations and weaknesses as possible. At the end of a CMMP assessment, a report containing tailored advice and recommendations, based on assessment findings, is provided to the organisation. CMMP has helped federal, state and territory government organisations understand their cyber security posture, their weaknesses and their strengths. As a result of CMMP assessments, hundreds of critical security vulnerabilities and weaknesses have been remediated.

**The Cyber Security Aftercare Program** (CSAP) ensures ASD maintains contact with prioritised government organisations and is able to assist them to achieve cyber security uplift. Under CSAP, ASD reaches out to government organisations on a regular basis to see how they are tracking against their Essential Eight+Sprint or CMMP report and offer services and assistance through the CURP if required. The CSAP provides government organisations with a high-level overview of other ASD programs and connects government organisations with relevant teams for further support.



**The National Exercise Program** helps critical infrastructure 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, and operational and technical capabilities.

### Case study 16: DeliverEx

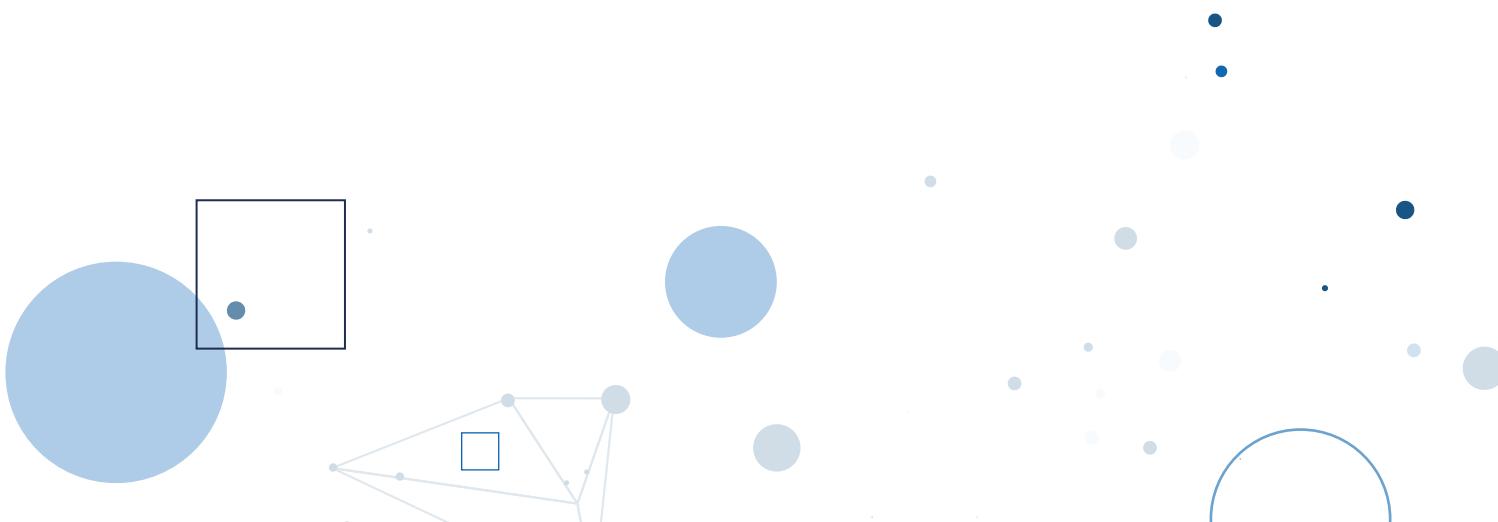
In 2023, ASD coordinated a national cyber security exercise series, known as DeliverEx, in partnership with Australian critical infrastructure owners and operators. The DeliverEx series strengthened industry and government's coordinated approach to cyber resilience, bringing together over 60 organisations from across Australia's transport and logistics sector, as well as government agencies responsible for transport and cyber security.

The DeliverEx series led engagement at the organisational, jurisdictional and executive levels:

- Organisational exercises – ASD supported registered organisations to enhance their cyber preparedness and resilience by providing a cyber security exercise package for them to conduct internal functional cyber security exercises.
- Jurisdictional exercises – ASD developed six voluntary discussion exercises to strengthen each state and territory's cyber security incident response arrangements for transport and logistics, which attracted 149 participants from 57 organisations. Industry, government and law enforcement participants explored how they would respond to a significant cyber security incident affecting multiple organisations within the sector concurrently.
- Executive discussion exercise – ASD invited 28 senior representatives from industry and government to attend a discussion exercise focused on strategic-level responsibilities, obligations, strategic decision-making and communications during a nation-wide cyber security incident affecting the transport and logistics sector.

Registered organisations were also provided with access to cyber security information sessions, exercise management training and technical capability development courses.

The exercise series supported organisations in validating their cyber security incident response plans and procedures required when responding to a cyber attack.



**The Australian Protective Domain Name System** (AUPDNS) is an opt-in security service available to all federal, state and territory government organisations to protect infrastructure from known malicious cyber activity. Information from AUPDNS directly assists the mission of ASD to build a national cyber threat picture that, in turn, is shared with its partners, including individuals, businesses, academia, and not-for-profit and government organisations.

**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 and assets using objective and data-driven approaches. The program relies on a mixture of open source, commercial and directly collected data.

CHIPs report findings through senior officers and operational teams in federal, state and territory governments to allow those organisations to better understand their online presence and improve their cyber hygiene. In addition to scanning for long-term improvement solutions to cyber hygiene and posture, CHIPs also conducts targeted open-source data collection in response to certain circumstances and events – referred to as High-priority Operational Tasking. Timely notifications from CHIPs are preventing cyber security incidents but also help with proactive incident discovery, before the adversary is fully embedded in a system.

CHIPs was expanded to include critical infrastructure organisations in November 2023. In FY2023–24, approximately 670 critical infrastructure organisations have been onboarded to the program from across priority sectors, including energy, financial services and markets, transport, and water and sewerage.

**The Cyber Threat Intelligence Sharing Platform** (CTIS) shares indicators of compromise (IOCs) in real-time within a growing community of Australian government and industry partners. CTIS also supports community partners to share their threat intelligence. Co-designed with industry, CTIS alerts security operations centre analysts to threats targeting Australian organisations.

In March 2024, the Australian Government announced a world-first initiative between ASD and Microsoft which enabled ASD's CTIS platform to connect with Microsoft's Sentinel platform. This connection extended the reach of CTIS through the creation of the CTIS/Sentinel plug-in capability that enable users of Microsoft's Sentinel platform to share IOCs directly into the CTIS platform. This collaboration supports organisations with their own ICT security teams to drive up their visibility of online threats, sharing data about malicious cyber activity with other industry partners.

## Case study 17: CTIS disrupts malicious infrastructure targeting users of an Australian tolling service

In March 2024, ASD detected fraudulent activities targeting users of an e-TAG tolling service in Australia. Investigative efforts revealed a significant number of domains impersonating the tolling service to deceive Australians with fraudulent fees and bills.

Malicious cyber actors employed SMiShing tactics, utilising SMS to deceive users into clicking on fraudulent links. A phishing kit, linked to a malicious cyber actor, was identified. The kit was being distributed by various resellers and targeting organisations globally. Through CTIS, ASD analysed and categorised the malicious infrastructure, and shared indicators of compromise (IOCs) with telecommunications providers for mitigation purposes. A domain takedown request issued by ASD led to the swift removal of the fraudulent domains, preventing further fraud.

Collaboration among cyber security agencies, telecommunications providers and website administrators helped to safeguard the Australian public from this malicious cyber activity. Continued vigilance and proactive measures are vital for maintaining digital security.

**The National Cyber Security Committee** (NCSC) is the mechanism for inter-jurisdictional coordination for cyber security incident response. The NCSC is co-chaired by the Head of the Australian Cyber Security Centre and a cyber security lead from a state or territory. The NCSC provides strategic coordination of national government preparedness and response efforts – including the exchange of threat information, assisting with consequence management activities and determining the National Cyber Security Arrangements level.

## Case study 18: NCSC at work

In early 2024, ASD, along with our Five Eyes partners, became aware of a vulnerability relating to certain Palo Alto PAN-OS firewall products. If exploited, a malicious cyber actor could attack the firewalls that were protecting many systems operated by business and government, both in Australia and worldwide.

ASD provided a timely classified threat brief for the NCSC. The close working relationship of agencies also allowed Australian government agencies to quickly identify any instances of exploitation on their systems.

Cyber threats impact business, government and the Australian economy across many jurisdictions. However, this case study demonstrates the value of close working relationships – with Five Eyes partners and Australian federal, state and territory governments. Forums such as NCSC allow Australian governments to leverage resources and bring together intelligence and technical expertise to protect Australia's national security interests and respond to significant cyber security incidents.

ASD publicly released a critical cyber security alert on the issue with technical information directed at the ICT teams of organisations and government. The alert, *OS Command Injection Vulnerability in GlobalProtect Gateway*, is available at [cyber.gov.au](http://cyber.gov.au).

# Supporting Australia during a cyber security incident

## Our role

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

### Report a cybercrime or cyber security incident

Report at [cyber.gov.au/report](https://cyber.gov.au/report) or call the 24/7 Australian Cyber Security Hotline on 1300 CYBERI (1300 292 371).

### Cybercrime

Cybercrime reports are automatically referred to the relevant state or territory law enforcement agency.

### Cyber security incidents

All cyber security incidents should be reported via the ReportCyber portal. A cyber security incident does not have to be a confirmed compromise to be reported and could include:

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

For ASD to help you effectively, we may request:

- indicators of compromise
- logs
- memory dumps
- disk information
- network traffic captures
- other analysis or reporting products.

### How ASD can help

When you report, ASD 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 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. They will work alongside you to liaise and coordinate technical briefings with other government agencies or industry partners to support your response. This could include federal, state, and/or territory government chief information security officers, federal law enforcement and international cyber partners
- 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. These products will be provided by ASD on a case-by-case basis
- an introduction to different areas within ASD for additional support, such as cyber resilience uplift activities and, if requested, assist you to contact the Department of Home Affairs or Australian Federal Police.



## How your reporting matters

ASD uses 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. Some of these products include:

- advisories published on ASD Partner Portal
- alerts and advisories published on [cyber.gov.au](https://cyber.gov.au)
- the Annual Cyber Threat Report.

## Your confidentiality is paramount

ASD is not a regulator and does not share any information provided by you without your express consent. Only information about the cyber security incident is captured when you report.

During FY2023–24, ASD monitored cyber threats across the globe 24 hours a day, 365 days a year, to alert Australians to cyber threats, provide advice and assist with incident response. ASD is a hub for private and public sector collaboration and information-sharing on cyber security, to prevent and combat threats and minimise harm to Australians.

The advice and assistance of ASD is for everyone, including critical infrastructure organisations, federal, state, territory and local governments, small and medium businesses, academia, not-for-profit organisations and the broader Australian community.



# Notes

## Sources

ASD manages or uses a number of 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 two distinct datasets: cybercrimes reported to law enforcement through ReportCyber, and cyber security incidents responded to by ASD. Data has been extracted from live datasets of cybercrime and cyber security reports disclosed to ASD. 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 will not reflect all cyber threats and trends in Australia's cyber security environment.

ASD encourages the reporting of cybercrimes, cyber security incidents and vulnerabilities to inform ASD 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, and can be viewed at: <https://www.cyber.gov.au/learn-basics/view-resources/glossary>.





