Australian Government
Australian Signals Directorate

AFP
AUSTRALIAN FEDERAL POLICE

AUSTRALIAN CRIMINAL INTELLIGENCE COMMISSION

ACSC Annual Cyber Threat Report

1 July 2020 to 30 June 2021

ACSC Australian Cyber Security Centre

cyber.gov.au

ACSC Australian Cyber Security Centre

Table of Contents

About the ACSC

The Australian Cyber Security Centre (ACSC) within the Australian Signals Directorate (ASD) leads the Australian Government's efforts on national cyber security. The ACSC brings together cyber security capabilities from across the Australian Government to improve the cyber resilience of the Australian community and help make Australia the most secure place to connect online. ACSC services include:

- the Australian Cyber Security Hotline, which is contactable 24 hours a day, seven days a week, via **1300 CYBER1 (1300 292 371)**. The Hotline provides advice and assistance to Australian organisations impacted by cyber security incidents
- advice and information about how to protect yourself and your business online via our website and the ACSC's Partner Portal
- alerts, technical advice, advisories and notifications to vulnerable organisations for significant cyber security threats
- cyber threat monitoring, and working with our partners domestically and globally, to share threat intelligence and counter cyber security threats
- a national footprint of Joint Cyber Security Centres (JCSCs) that supports ACSC collaboration with over 1,750 business, government, law enforcement and academic partners on cyber security issues
- uplift activities to enhance cyber security resilience for Australian organisations.

The ACSC acknowledges the contributions from Commonwealth, state and territory government agencies, law enforcement and industry organisations in developing this report.

About the contributors

Australian Government
Australian Signals Directorate

ASD is a member of Australia's National Security Community and works across intelligence, cyber security and offensive operations in support of the Australian Government and the Australian Defence Force (ADF). ASD's purpose is to defend Australia from global threats and help advance Australia's national interests. It does this by mastering technology to inform, protect and disrupt.

Australian Government
Department of Defence
Defence Intelligence Organisation

The Defence Intelligence Organisation (DIO) co-leads the ACSC's Cyber Threat Assessment team – in partnership and jointly staffed with ASD – to provide the Australian Government with an all-source, strategic, cyber threat intelligence assessment capability.

AUSTRALIAN CRIMINAL INTELLIGENCE COMMISSION

The Australian Criminal Intelligence Commission (ACIC), as Australia's national criminal intelligence agency, works with law enforcement partners to improve the nation's ability to respond to crime impacting Australia. The ACIC provides the Australian Government's cybercrime intelligence function within the ACSC. Its role in the ACSC is to provide cybercrime-related criminal intelligence insights by working closely with law enforcement, intelligence, and industry security partners in Australia and internationally.

AUSTRALIAN FEDERAL POLICE

The Australian Federal Police (AFP) is responsible for enforcing Commonwealth criminal law; contributing to combating complex transnational, serious, and organised crime impacting Australia's national security; and protecting Commonwealth interests from criminal activity in Australia and overseas. The AFP's cybercrime teams within the ACSC provide the AFP with the capability to collaborate with other ACSC partners, triage new referrals and complaints, undertake targeted intelligence development and coordinate law enforcement responses to cybercrimes of national significance.

Australian Government
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, people smuggling 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 the ACSC includes intelligence collection, investigations and intelligence-led outreach to business and government partners.

Australian Government
Department of Home Affairs

The Department of Home Affairs leads cyber security policy for the Australian Government, including Australia's Cyber Security Strategy 2020 and overseeing its implementation. Home Affairs outreach officers work in the ACSC's Joint Cyber Security Centres to work with small and medium businesses to help them uplift their cyber resilience.

About this report

The ACSC Annual Cyber Threat Report 2020–21 has been produced by the ACSC, with contributions from DIO, ACIC, AFP, ASIO, the Department of Home Affairs, and industry partners. The report covers the financial year from 1 July 2020 to 30 June 2021. This is the second unclassified annual cyber threat report since ASD became a statutory agency in July 2018.

The report highlights the key cyber threats affecting Australian systems and networks, and uses strategic assessments, statistics, trends analysis, and case studies to describe the nature, scale, scope and impact of malicious cyber activity affecting Australian networks. It also provides advice to Australian individuals and organisations on what they can do to protect their networks from cyber threats.

Information, sources and data

The ACSC manages and accesses a number of unique data holdings to ensure tailored advice and assistance to Australian governments, organisations and the public. ACSC data used in this report has been extracted from live datasets of cybercrime reports and cyber security incidents reported to the ACSC. 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 the ACSC may not reflect all cyber threats and trends in Australia's cyber security environment.

The ACSC encourages the reporting of cyber security incidents and cybercrimes to inform ACSC advice and assistance to vulnerable organisations, and enhance situational awareness of the national cyber threat environment.

Glossary of key cyber terminology

The ACSC glossary for terminology used in reports can be found on the website:
https://www.cyber.gov.au/acsc/view-all-content/glossary

Feedback

The ACSC welcomes feedback to improve the reports and services it provides to Australians. Feedback can be provided by emailing asd.assist@defence.gov.au or via phone at **1300 CYBER1 (1300 292 371).**

Executive summary

Over the 2020–21 financial year, Australian individuals, organisations and government entities' engagement online was largely influenced by the impacts of the COVID-19 pandemic. The pandemic has significantly increased Australian dependence on the internet – to work remotely, to access services and information, and to communicate and continue our daily lives. This dependence has increased the attack surface and generated more opportunities for malicious cyber actors to exploit vulnerable targets in Australia.

Over the 2020–21 financial year, the ACSC received over 67,500 cybercrime reports, an increase of nearly 13 per cent from the previous financial year. The increase in volume of cybercrime reporting equates to one report of cyber attack every 8 minutes compared to one every 10 minutes last financial year. A higher proportion of cyber security incidents this financial year was categorised by the ACSC as 'substantial' in impact. This change is due in part to an increased reporting of attacks by cybercriminals on larger organisations and the observed impact of these attacks on the victims, including several cases of data theft and/or services rendered offline. The increasing frequency of cybercriminal activity is compounded by the increased complexity and sophistication of their operations. The accessibility of cybercrime services – such as ransomware-as-a-service (RaaS) – via the dark web increasingly opens the market to a growing number of malicious actors without significant technical expertise and without significant financial investment.

No sector of the Australian economy was immune from the impacts of cybercrime and other malicious cyber activity. Government agencies at all levels, large organisations, critical infrastructure providers, small to medium enterprises, families and individuals were all targeted over the reporting period – predominantly by criminals or state actors.

The ACSC identified the following key cyber security threats and trends in the 2020–21 financial year:

- **Exploitation of the pandemic environment:** Malicious actors exploited the coronavirus pandemic environment by targeting Australians' desire for digitally accessible information or services. For example, spear phishing emails were regularly associated with COVID-related topics, encouraging recipients to enter personal credentials for access to COVID-related information or services. Criminal and state actors also targeted the health care sector. State actor activity was probably motivated by access to intellectual property or sensitive information about Australia's response to COVID, while criminals sought to leverage critical services to increase the motivation of victims to pay ransoms. For example, the health care sector was a significant target of ransomware attacks during the reporting period.

- **Disruption of essential services and critical infrastructure:** Approximately one quarter of cyber incidents reported to the ACSC during the reporting period were associated with Australia's critical infrastructure or essential services. Significant targeting, both domestically and globally, of essential services such as the health care, food distribution and energy sectors has underscored the vulnerability of critical infrastructure to significant disruption in essential services, lost revenue and the potential of harm or loss of life.

- **Ransomware** has grown in profile and impact, and poses one of the most significant threats to Australian organisations. The ACSC recorded a 15 per cent increase in ransomware cybercrime reports in the 2020–21 financial year. This increase has been associated with an increasing willingness of criminals to extort money from particularly vulnerable and critical elements of society. Ransom demands by cybercriminals ranged from thousands to millions of dollars, and their access to darkweb tools and services improved their capabilities. Extortion tradecraft evolved, with criminals combining the encryption of victim networks with threats to release or on-sell stolen sensitive data and damage the victim's reputation. Ransomware incidents disrupted a range of sectors, including professional, scientific and technical organisations, and those in health care and social assistance. The global impact of the Colonial Pipeline and JBS Foods attacks underscores the potential debilitating and widespread impact of ransomware attacks.

- **Rapid exploitation of security vulnerabilities:** State and criminal cyber actors continued to compromise large numbers of organisations by prosecuting publicly disclosed vulnerabilities at speed and scale. Malicious actors exploited security vulnerabilities, at times within hours of public disclosure, patch release or technical write up – particularly if proof of concept (PoC) code that identified the vulnerabilities in systems was also released.

- **Supply chains** – particularly software and services – continue to be targeted by malicious actors as a means to gain access to a vendor's customers. Although the consequences of major supply chain attacks – such as SolarWinds – were not as severe for Australia, a number of organisations were forced to take mitigation actions to prevent more serious impacts to their networks. The threat from supply chain compromises remains high – it is difficult for both vendors and their customers to protect their networks against well-resourced actors with the ability to compromise widely used software products.

- **Business email compromise (BEC)** continues to present a major threat to Australian businesses and government enterprises, especially as more Australians work remotely. In the 2020–21 financial year, the average loss per successful event has increased to more than $50,600 (AUD) – over one-and-a-half times higher than the previous financial year. Cybercriminal groups conducting BEC have likely become more sophisticated and organised, and these groups have developed enhanced, streamlined methods for targeting Australians.

ACSC Australian Cyber Security Centre

During the 2020–21 financial year,

The ACSC observed

Over **67,500** cybercrime reports, an increase of nearly **13%** from the previous financial year

Self-reported losses from cybercrime totalling more than **$33 billion**

Approximately **one quarter** of reported cyber security incidents affected entities associated with Australia's critical infrastructure

Over **1,500** cybercrime reports per month of malicious cyber activity related to the coronavirus pandemic (approximately 4 per day)

More than **75%** of pandemic-related cybercrime reports involved Australians losing money or personal information

Nearly **500** ransomware cybercrime reports, an increase of nearly **15%** from the previous financial year

Fraud, online shopping scams and online banking scams were the top reported cybercrime types

An increase in the average severity and impact of reported cyber security incidents, with nearly half categorised as ‘substantial’

ACSC Australian Cyber Security Centre

What the ACSC has done

Published **27** alerts and **12** advisories to cyber.gov.au – which saw more than **7.8 million** visits

Published more than **40** step-by-step guides to support older Australians, families and businesses to implement sound cyber security practices

Expanded the Partnership Program to include three tiers of membership: Network, Business, and Home

- ACSC now has more than **1,700** network partners, **2,000** business partners, and **tens of thousands** of home partners

Supported **18** cyber security exercises involving over **50** organisations to strengthen Australia's cyber resilience

Launched the CI-UP pilot to help protect Australia's most critical systems

Grew the active Information Security Registered Assessors Program (IRAP) with the number of assessors grown by more than **20%** since the program reopened in January 2021

ACSC Australian Cyber Security Centre

What the ACSC has done

Received over **22,000** calls on the Cyber Security Hotline – an average of **60** per day and an increase of more than **310%** from the previous financial year

Provided advice or assistance to over **1,630** cyber security incidents

Undertook **34** high-priority operational tasking activities in response to identified and potential cyber threats or significant events – this included scanning for vulnerable Australian devices

Removed over **7,700** websites that were hosting cybercrime activity from the internet

Signed up **16** Australian Government agencies to the Australian Protective Domain Name Service, processing more than **5.5** billion queries and blocking over **400,000** malicious domain requests

Disrupted over **110** malicious COVID-19 themed websites, with assistance from Telstra and Services Australia

What you should do

Given the cyber threat landscape over the past year, the ACSC continues to recommend all Australian organisations prioritise implementation of the Essential Eight Maturity Model and, in particular, consider the following six actions:

Report all cybercrime and cyber security incidents, via ReportCyber. This is the central place to report a cyber security incident, cybercrime, or a cyber security vulnerability. The ACSC website (cyber.gov.au) provides extensive advice, guidance and information on a range of cyber security matters. The website also provides additional assistance and referral pathways depending on the nature of the incident or cybercrime. The ACSC encourages the reporting of cyber security matters to assist the ACSC in understanding the Australian cyber threat environment.

Become an ACSC Partner. Australian organisations who partner with the ACSC receive threat insights, advisories and advice to enhance their situational awareness. Cyber security professionals in our partner organisations also receive collaboration opportunities across industry and the Australian Government.

Know your networks. The ACSC encourages all users to understand and review their networks to establish where valuable or sensitive information and infrastructure is located, and apply appropriate cyber security measures proportionate to the risk of compromise.

Patch within 48 hours where an exploit exists. Malicious cyber actors monitor reporting of security vulnerabilities and use automated tools to regularly scan for and exploit network vulnerabilities. This means that organisations can no longer follow monthly patch update cycles, and should prioritise patching to protect their networks from cyber security incidents. Ensure patches, updates or vendor mitigations for security vulnerabilities in internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists. Where this is not possible, it is important that organisations have robust cyber incident detection and response plans in place. For organisations that cannot patch their internet-facing services in a very timely manner, adopting trustworthy Software as a Service (SaaS) or Platform as a Service (PaaS) cloud approaches to internet-facing services, which immediately apply patches on the customer's behalf, may assist.

Evaluate risks associated with cyber supply chains. The ACSC encourages organisations to follow the ACSC's advice on cyber supply chain risk mitigation.

Prepare for a cyber security incident by having incident response, business continuity and disaster recovery plans in place, and testing them. An incident response plan enables organisations to respond decisively to a cyber security incident, limit its impact and support recovery. Testing the incident response, business continuity and disaster recovery plans, including through cyber security exercises involving restoration of systems, software and important data from backups, provides an opportunity to review and improve in a controlled environment.

Cybercrime and cyber security incident statistics

Cybercrime and cyber security incident statistics

Report cybercrime and cyber security incidents

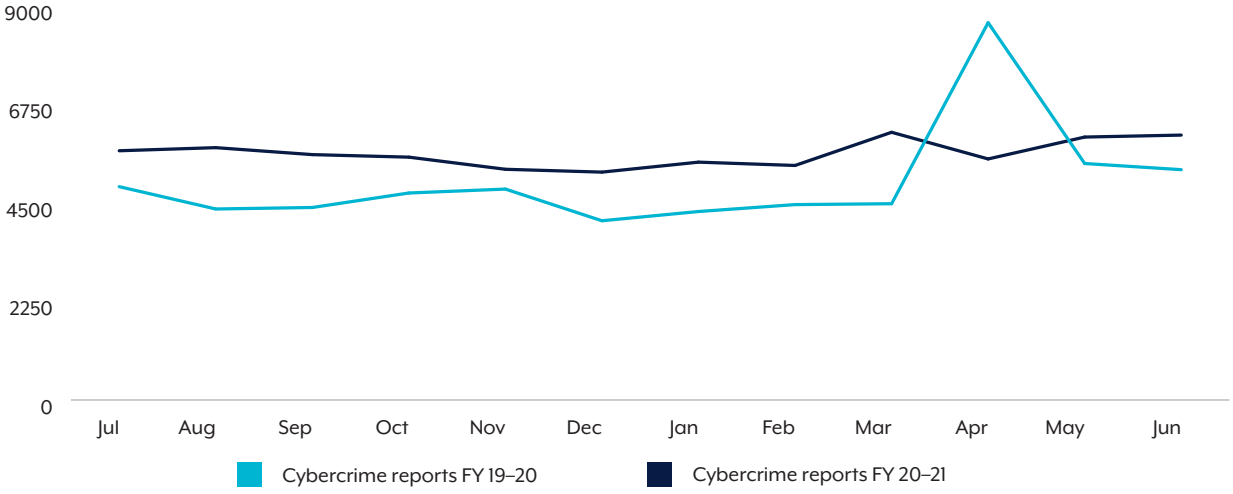
A cybercrime or cyber security incident can cause financial and reputational damage, disrupt business and critical services, and result in further or ongoing malicious activity to an organisation. While the costs of impacts are difficult to quantify, the costs of remediation for a cybercrime or cyber security incident can be far greater than early and ongoing investment in prevention.

The ACSC encourages the reporting of all cybercrime and cyber security incidents, via ReportCyber. This is the central place to report a cyber security incident, cybercrime, or a cyber security vulnerability. The ACSC is contactable via email at asd.assist@defence.gov.au or through the Australian Cyber Security Hotline on **1300 CYBER1 (1300 292 371)**. The hotline provides advice and assistance to Australians impacted by cyber security incidents.

Cybercrime statistics

During the 2020–21 financial year, over 67,500 cybercrime reports were made via ReportCyber, an increase of nearly 13 per cent from the previous financial year (see Figure 1). One cybercrime report is made approximately every eight minutes in Australia.

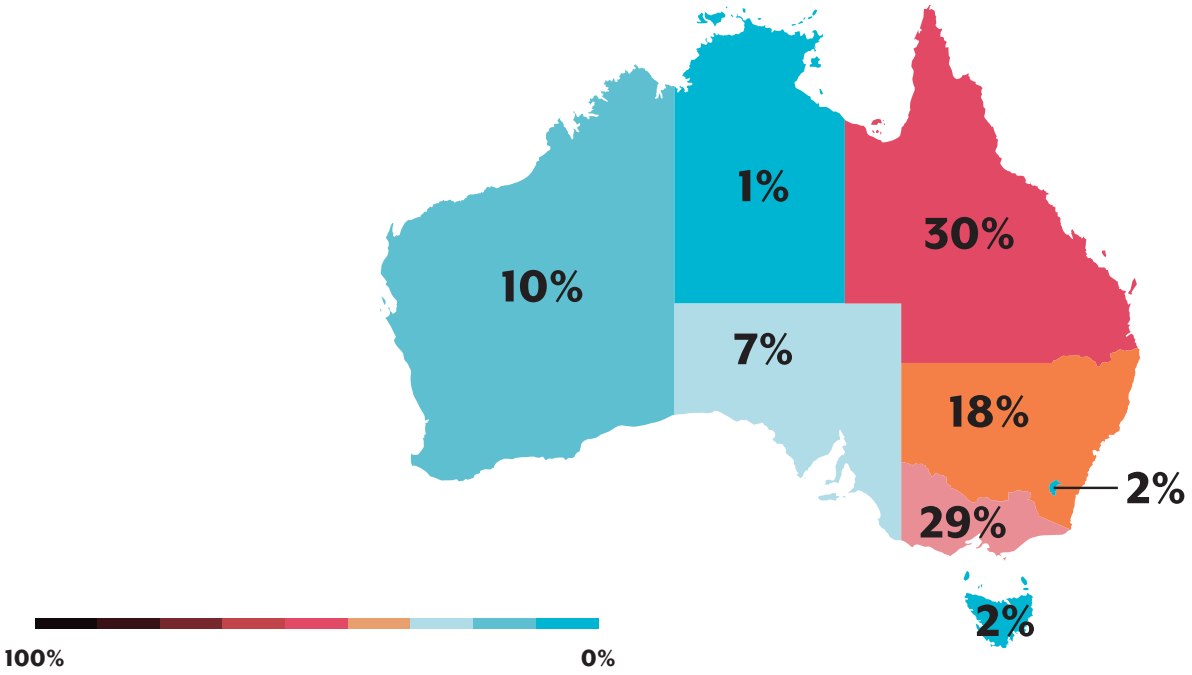
Figure 1: Cybercrime reports by month for financial year 2020–21 compared with financial year 2019–20



Note: The notable spike in April 2020 relates to a bulk extortion campaign, resulting in nearly half of the cybercrime reports for that month.

Australia's larger capital centres on the eastern seaboard, where a majority of the Australian population and companies are located, continue to be the main areas for reported cyber security incidents and cybercrime activity (see Figure 2). The highest proportion of cybercrime reports made in the 2020–21 financial year were made from entities or individuals in Queensland and Victoria, accounting for approximately 30 per cent each. While a lower number of reports were made overall, the highest average financial losses were self-reported by victims located in South Australia and Western Australia.

Figure 2: Breakdown of cybercrime incidents by assigned jurisdiction for financial year 2020–21

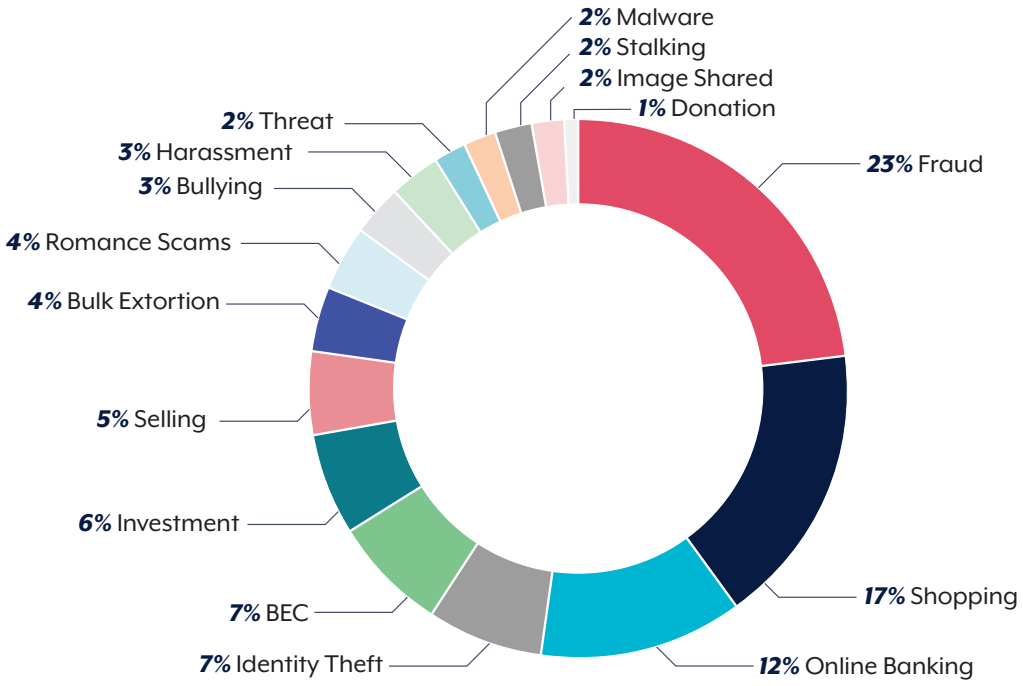


Fraud-related cybercrime – where actors use computers or online services to commit fraud – continued to be a prevalent cyber threat to Australians, with this activity accounting for nearly 23 per cent of cybercrime reports (see Figure 3). The cybercrime categories with the most reports were primarily types of cyber-enabled crime, which occur when computers are used to facilitate an existing offence such as online fraud or online child sexual exploitation offences. The top three cybercrime types reported via ReportCyber were:

- fraud cybercrime – approximately 23 per cent
- shopping cybercrime – approximately 17 per cent
- online banking cybercrime – approximately 12 per cent.

While the number of ransomware-related cybercrime reports is a relatively small proportion of the total number of cybercrime reports, ransomware remains the most serious cybercrime threat due to its high financial impact and disruptive impacts to victims and the wider community.

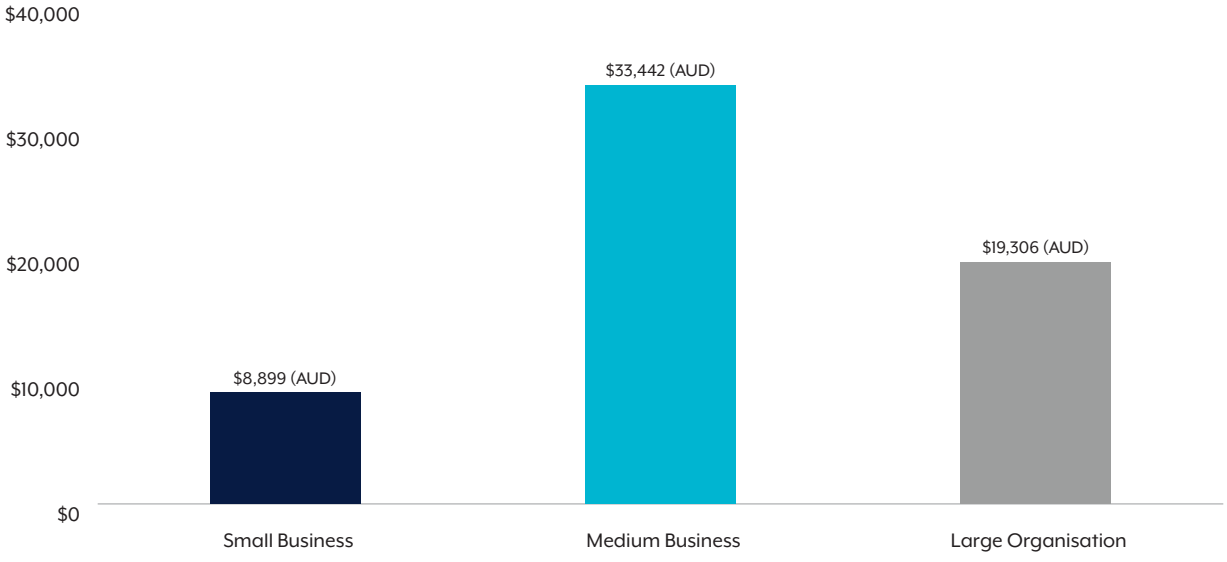
Figure 3: Cybercrime reports by type for financial year 2020–21



Note: Percentages rounded to the nearest whole number.

Self-reported financial losses due to cybercrime in Australia-based cybercrime reports totalled more than $33 billion (AUD). Due to open and complex cybercrime investigations, these figures may not be fully verified by law enforcement and a significant portion are related to cyber-enabled crimes. Small businesses made a higher number of cybercrime reports than in the previous financial year; however, medium businesses had the highest average financial loss per cybercrime report (see Figure 4).

Figure 4: Cybercrime reports and average reported loss by organisation size for financial year 2020–21



Note: Figures rounded to the nearest dollar (AUD).

ACSC cyber security alerts and advisories

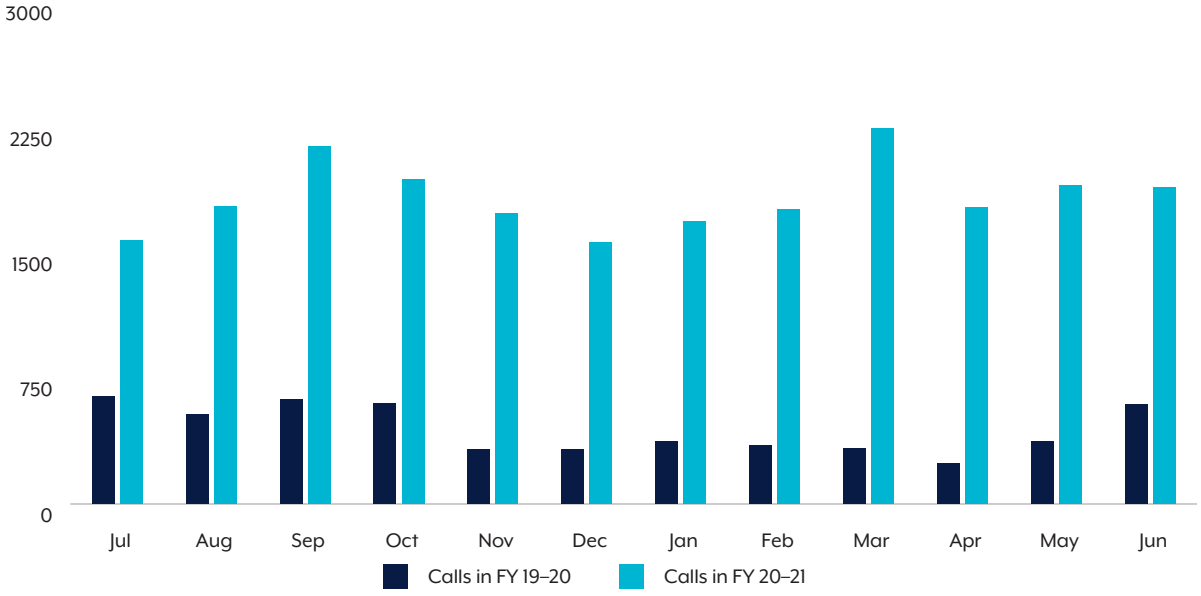
During the 2020–21 financial year, the ACSC publicly released:

- 27 alerts providing critical information that enabled early identification and prevention of cyber security threats. Alerts can be found on the ACSC's website.
- 12 advisories providing detailed advice on significant cyber security threats. Advisories can be found on the ACSC's website.

Calls to the ACSC via 1300 CYBER1

Since the start of the 2020–21 financial year, the ACSC has seen a significant increase in the number of calls to 1300 CYBER1. The number of calls in the 2020–21 financial year totalled more than 22,000, an average of 60 calls received per day. This is an increase of more than 310 per cent, compared with the previous financial year where the ACSC received 5,300 calls (see Figure 5). This is largely attributable to an increase in public awareness of cyber security matters resulting in Australians contacting the ACSC for general cyber security advice and assistance as well as an increase in cybercrime reporting.

Figure 5: Call volumes for financial year 2020–21 compared with financial year 2019–20



ACSC cyber security incidents

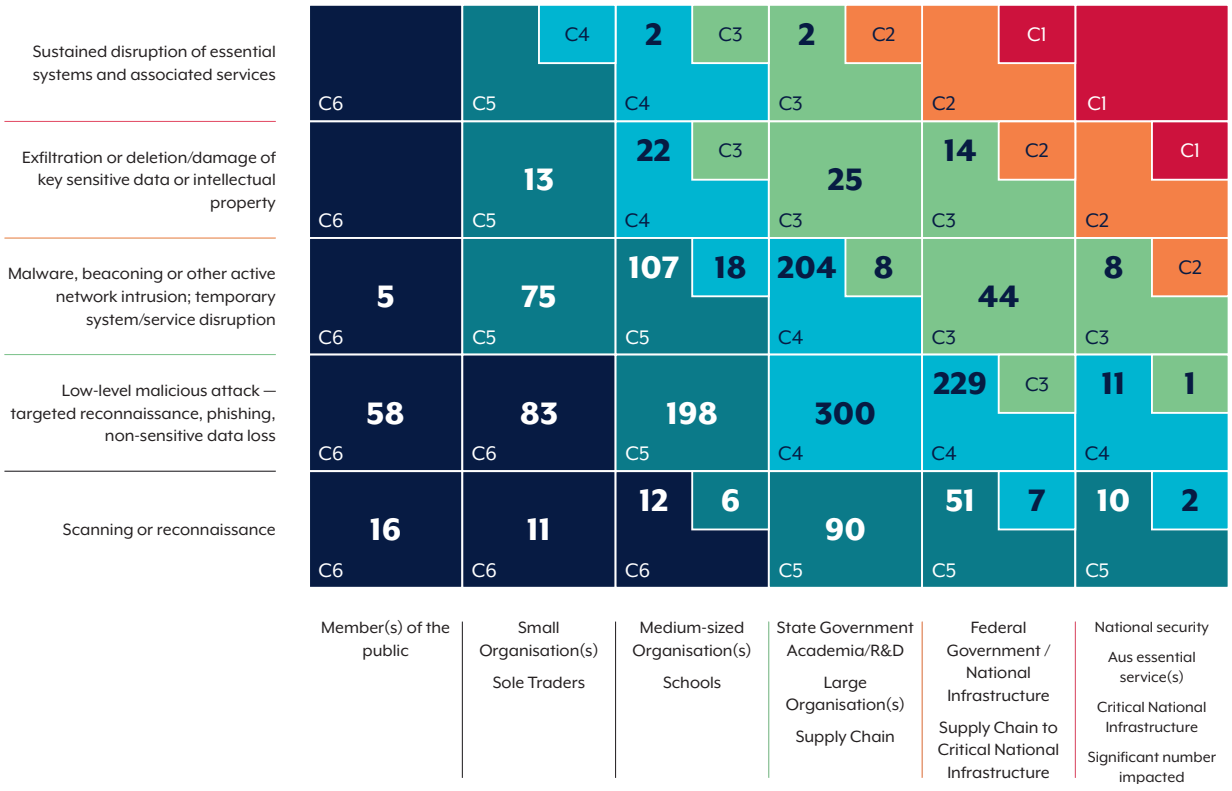
The ACSC categorises each incident it responds to on a scale of Category 1, the most severe, to Category 6, the least severe. During the 2020–21 financial year, the ACSC responded to approximately 1,630 cyber security incidents, an average of 31 cyber security incidents per week.

Compared to the previous financial year, the total number of cyber security incidents in the 2020–21 financial year decreased by 28 per cent and there were no Category 1 or Category 2 incidents in the 2020–21 financial year. However, a higher proportion of incidents in the 2020–21 financial year were categorised as Category 4 incidents – indicating that cyber security incidents reported this year had a more profound impact on victim organisations. This change is due in part to an increase in attacks by cybercriminals on larger organisations and the impact of these attacks on the victims. The attacks included data theft, extortion and/or rendering services offline.

Category 4 incidents accounted for nearly half (49 per cent) of the reported cyber security incidents in the 2020–21 financial year (see Figure 6). This is a change from the previous financial year, where the highest proportion of cyber security incidents was at Category 5 (36 per cent), and Category 4 cyber security incidents accounted for only a third of total cyber security incidents (35 per cent).

The highest proportion of incidents the ACSC responded to related to low-level malicious activity such as targeted reconnaissance, phishing, or non-sensitive data loss, accounting for more than half of the cyber security incidents.

Figure 6: Cyber security incidents by incident category for financial year 2020–21

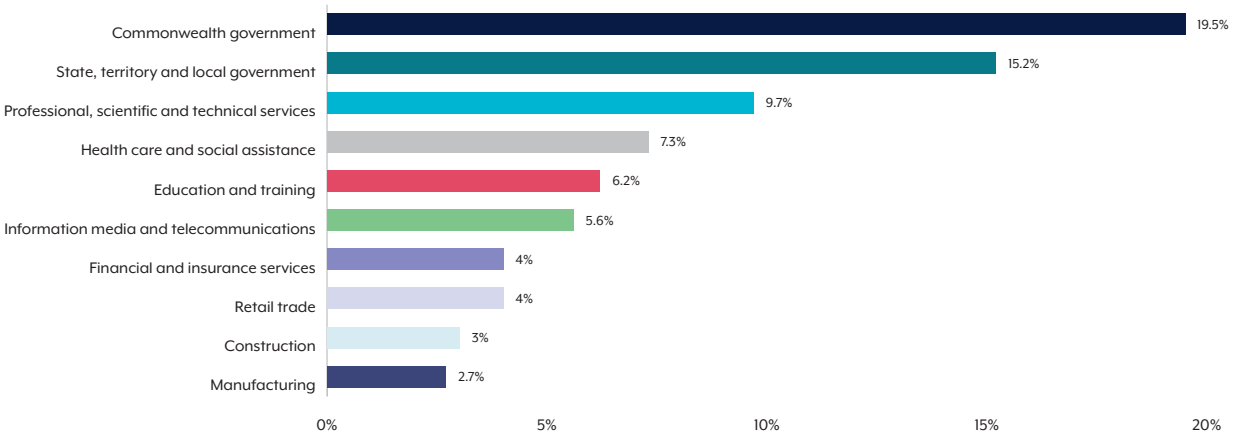


Note: In order to manage the range and volume of reported incidents, the ACSC uses a cyber incident categorisation system to triage and prioritise responses to mitigate each incident. The ACSC categorises incidents based on severity of impact and extent of compromise. This allows the ACSC to focus its resources more effectively, and ensures a consistent approach and an appropriate level of response measures to each incident.

Approximately one quarter of reported cyber security incidents affected critical infrastructure organisations, including essential services such as education, health, communications, electricity, water and transport. After the government sectors as the top reporting sectors, the professional, scientific and technical sector and the health care and social assistance sector reported the highest number of cyber security incidents during the 2020–21 financial year. The top ten reporting sectors accounted for approximately 77 per cent of all incidents for the 2020–21 financial year (see Figure 7).

The ACSC is working closely with critical infrastructure organisations and industry partners to improve information sharing on the scale and scope of cyber security incidents affecting Australia (refer to the CTIS Platform section for more information).

Figure 7: Cyber security incidents by the top ten reporting sectors for financial year 2020–21



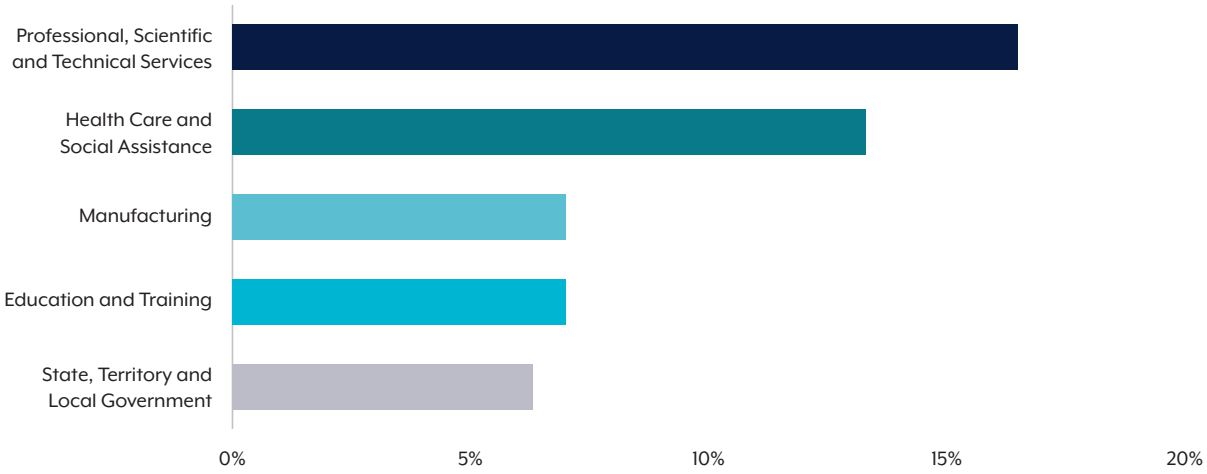
Note: While Commonwealth, state, territory, and local government accounted for approximately one third (35 per cent) of incidents in the 2020–21 financial year, the high reporting frequency of government agencies is in part due to the obligation to report significant cyber security incidents to the ACSC, and may not necessarily reflect an increased susceptibility of these networks to cyber incidents, when compared with industry.

Ransomware

During the 2020–21 financial year, the ACSC received nearly 500 ransomware cybercrime reports via ReportCyber, which is an increase of nearly 15 per cent compared with the previous 2019–20 financial year.

In the 2020–21 financial year, the ACSC also responded to nearly 160 cyber security incidents related to ransomware. The professional, scientific and technical services sector and the health sector reported the most ransomware-related cyber security incidents (see Figure 8). The top five reporting sectors for ransomware-related incidents accounted for approximately 50 per cent of all ransomware-related incidents reported to the ACSC during the 2020–21 financial year.

Figure 8: Top five reporting sectors for ransomware-related cyber security incidents

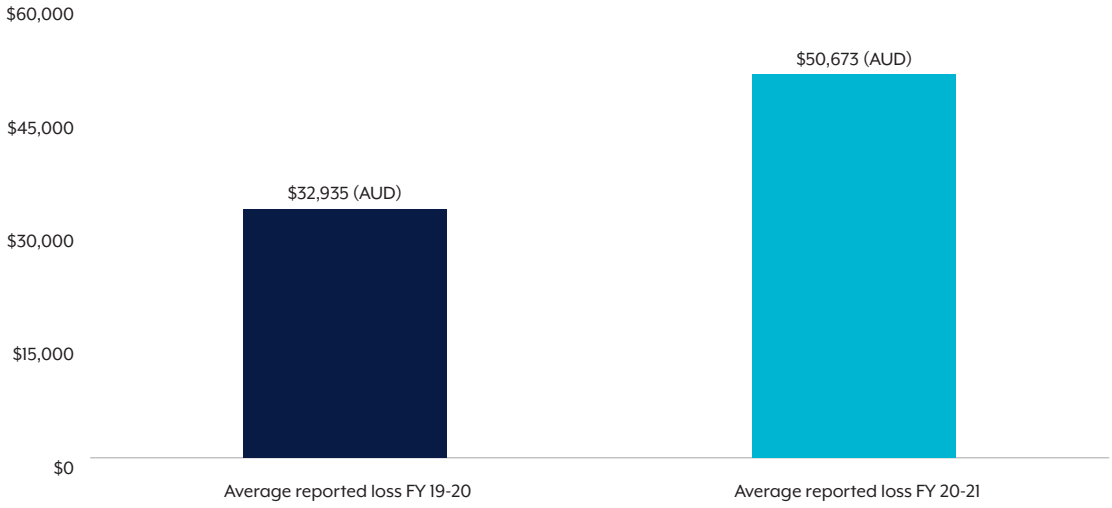


Phishing campaigns, targeted spear phishing, remote access through vulnerable machines and the use of publicly available exploits remain the most common vectors for deploying ransomware. Personal information on professional and social networking platforms, including profiles, can provide malicious actors with useful information for targeting, including spear phishing or other socially engineered online approaches.

Business Email Compromise (BEC)

Australian businesses are losing significant amounts of money through BEC. BEC cybercrime was one of the top cybercrime categories, making up nearly 7 per cent of the cybercrime reports received in the 2020–21 financial year. While there has been a slight decrease in BEC reports compared with the previous financial year, self-reported financial losses have increased – total losses were approximately $81.45 million (AUD) for the 2020–21 financial year, an increase of nearly 15 per cent from the previous financial year. Average loss per successful BEC transaction also increased, by 54 per cent (see Figure 9) – in one case, BEC led to the bankruptcy of a company (see Case Study: Australian hedge fund subject to BEC and declared bankruptcy, page 45).

Figure 9: Average reported losses per successful BEC cybercrime report made in financial year 2020–21 compared with financial year 2019–20



Note: Figures rounded to the nearest dollar (AUD).

Threat environment and key cyber security trends

Threat environment and key cyber security trends

Australia faced a complex and evolving cyber threat environment in 2020 and 2021. This was in part due to the impacts of the coronavirus pandemic, but also to the increasing opportunities afforded to malicious actors, the rampant activities of cybercriminals and Australia's geostrategic environment.

The coronavirus pandemic continued to expand the boundaries of Australia's computer networks, pushing corporate systems into homes across the nation as a large percentage of the workforce shifted to remote working arrangements. The speed at which this occurred saw many organisations rapidly deploy new remote networking solutions, sometimes to the detriment of their cyber security. **Various malicious cyber actors** repeatedly took advantage of Australia's heightened vulnerability during this time to conduct espionage, steal money and sensitive data, and disrupt the services on which Australians rely.

Alongside the virtualisation of Australian life, the disclosure of significant vulnerabilities in software used in Australian networks expanded the targeting opportunities available to adversaries. The Microsoft Exchange and Accellion File Transfer Application (FTA) vulnerabilities were notable examples where the ACSC observed multiple compromises after initial disclosure. In some cases, both **state-sponsored actors and cybercriminals** were able to rapidly exploit vulnerabilities at scale, including against targets in Australia.

Across this period, Australia remained a key and regular target of **state-sponsored actors.** These actors employed a wide range of tactics to target Australian networks, seeking sensitive information that could be used to weaken Australia's competitive advantage and degrade national security.

Australians were also frequent victims of financially motivated cybercrime, particularly ransomware and business email compromise. **Cybercriminals** were prolific and overt in their targeting of Australian organisations, and the impacts of their operations were felt across the community. In some cases, these impacts included the disruption of essential services, as happened when the March 2021 ransomware attack against a Victorian public health service affected four hospitals and aged care facilities, and resulted in the postponement of elective surgeries. Ransomware attacks on an Australian media company and JBS Foods further demonstrated a move by **cybercriminals** away from low-level ransomware operations towards extracting hefty ransoms from large or high-profile organisations. To increase the likelihood of ransoms being paid, cybercriminals would encrypt networks and also exfiltrate data, then threaten to publish stolen information on the internet. These shifts in targeting and tactics have intensified the ransomware threat to Australian organisations across all sectors, including critical infrastructure.

Cybercriminals also preyed on the community's desire for information and resources on topical issues. In particular, the pandemic provided compelling content for email and SMS phishing campaigns. However, often poor cyber security controls – such as unpatched vulnerabilities and unsecured remote access solutions – allowed cybercriminals to launch their attacks with minimal targeting effort or technical expertise. The ease with which malicious actors could gain access to networks increased Australia's susceptibility to cybercrime targeting.

This was also a period in which new and serious concerns joined the list of existing cyber threats. Chief among these was the protection of Australia's COVID-19 vaccine supply, including distribution processes, from malicious cyber actors. State and criminal cyber actors alike possess the capability to disrupt Australia's critical infrastructure – including vaccine supply and distribution chains – with the pandemic only amplifying the opportunities for these actors to cause Australia harm. Even in the absence of direct and intentional targeting, there remains the potential for malicious cyber actors to inadvertently disrupt vaccine supply and distribution chains, making the threat more difficult to address.

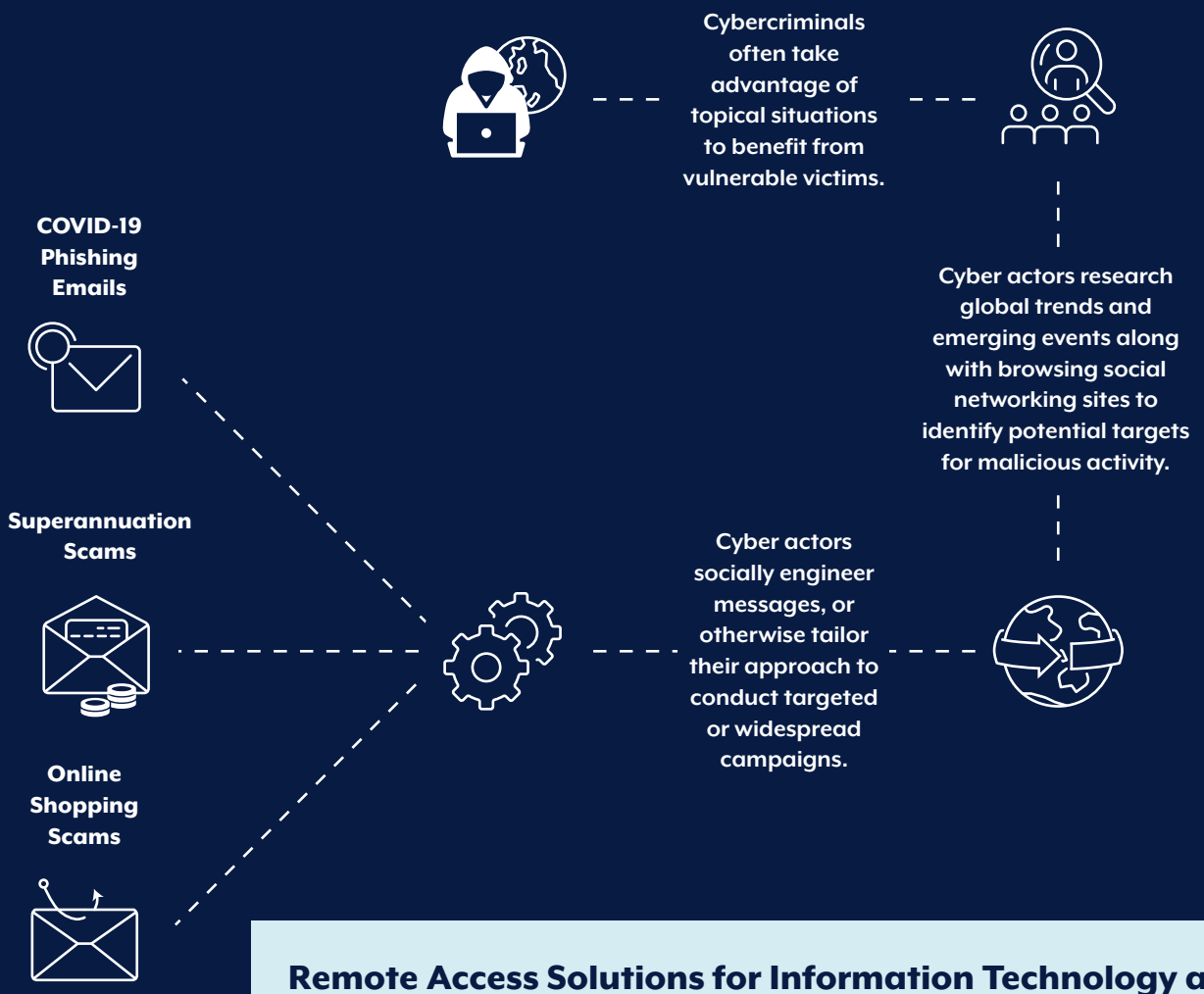
What does the future hold?

As we develop new ways of using technology in our lives and businesses, Australia will continue to experience significant cyber threats. Networks will grow in complexity and become more difficult to defend – fuelled in part by the rapid spread of the Internet of Things. At the same time, malicious cyber actors will continue to capitalise on old but effective methods to compromise victims, while also embracing new technologies to modernise and industrialise their operations, including the use of automated tools and techniques to exploit large numbers of victims.

The headlining global cyber security events of 2020 and 2021 – such as the SolarWinds Orion supply chain compromises, the exploitation of on-premises Microsoft Exchange server vulnerabilities and the volley of large-scale ransomware attacks – are now the new norm. Over the next 12 months, additional supply chain compromises will likely come to light, major vulnerabilities will continue to emerge and Australia will experience more major financially motivated cyber incidents, some of which could disrupt critical services.

Despite the headlines, many of the compromises experienced by Australians will continue to be fuelled by a lack of adequate cyber hygiene. This delivers a significant advantage to adversaries and lowers the technical barrier to targeting victims in Australia, highlighting the need to uplift cyber security maturity across the Australian economy. Given the prevalence of malicious cyber actors targeting Australian networks – which is often under-reported to the ACSC – there is a strong need for greater resilience, and for Australian organisations and individuals to prepare to respond to and recover from any cyber attack to their networks.

COVID-19 themed malicious activity



Remote Access Solutions for Information Technology and Operational Technology systems

Remote access is where an individual can gain access to a computer, device, or network remotely through an internet connection.

Before commencing remote access working arrangements, organisations should consider sufficient business continuity plans, best practices and alternative arrangements.

While remote access may be the best option, it also provides cyber actors with an additional avenue to access personal accounts and information, and once an actor is in the system, they can be difficult to remove. Cyber actors may have installed malware onto the system without a user knowing.

More information is available on COVID-19 and Remote Access Operational Technology Environments.

Trends in the COVID-19 environment

The coronavirus pandemic exposed Australia to heightened cyber threats, with the health sector and key entities involved in the supply of the COVID-19 vaccine placed at particular risk. Australian individuals and families received large volumes of malicious emails and text messages themed to the pandemic, while many organisations – including health services – suffered compromises at the hands of cybercriminals who sought to profit from the global crisis. At the same time, state-sponsored actors sought access to sensitive information relating to the pandemic, including vaccine research, increasing the threat of cyber espionage to Australia.

The ACSC has remained committed to protecting Australians from malicious cyber activity during this difficult time, including by disrupting cybercriminals operating offshore and working with industry partners to increase protective measures. From 1 July 2020 to 30 June 2021, the ACSC:

- received over 1,500 cybercrime reports per month of malicious cyber activity related to the coronavirus pandemic (approximately four per day), with more than 75 per cent of these relating to individual Australians reporting loss of finances or personal information to scams and online fraud
- received over 130 cybercrime reports related to entities involved in the COVID-19 response, and responded to nearly 120 cyber security incidents affecting health sector organisations
- disrupted over 110 malicious COVID-19 themed websites, with assistance from Australia's major telecommunications providers
- launched a pilot program in September 2020, in collaboration with Telstra and Services Australia, to identify and reject illegitimate phishing text messages that impersonate myGov and Centrelink before they reach Telstra customers (see the ACSC initiative: Collaboration with Telstra and Services Australia to combat malicious COVID-19 themed phishing, page 27)
- removed over 7,700 websites, since the service commenced in March 2021, that were hosting cybercrime activity from the internet (see ACSC initiative: Successful Takedown Notifications – COVID-19, page 28)
- successfully conducted offensive cyber operations to combat cybercrime originating outside Australia. The ACSC identified offshore cybercriminals capitalising on the impacts of the pandemic by targeting Australian households and businesses using COVID-19 themed device scams and other malicious cyber activities. These were successfully disrupted by disabling the cybercriminals' infrastructure and blocking their access to stolen information.

Trends in the health sector

Targeting of the health sector, particularly by cybercriminals, is one of the most significant cyber threats Australia has so far faced during the pandemic. The health sector in Australia reported the second highest number of cyber security incidents both overall and for ransomware-related cyber security incidents (see Figure 7 and Figure 8).

This threat only grew as COVID-19 vaccines were developed and the Australian health sector started to rely on entities involved in the vaccine supply chain. The enormous pressures the health sector faced in responding to the pandemic increased its susceptibility to cyber incidents, with malicious cyber actors likely viewing health organisations as more vulnerable during this time.

Malicious cyber activity against the European Medicines Agency in late 2020, followed by the early 2021 targeting of an offshore university lab studying COVID-19, served to highlight the potential threat to Australia's own vaccine supply chain. In tandem with this threat, the continued spate of ransomware attacks on health entities around the globe, including in Australia, demonstrated the tangible impacts cybercrime can have on critical infrastructure, particularly during a crisis. As a consequence of these attacks, medical staff were locked out of patient records, surgeries were delayed, and patients seeking emergency care were diverted to other facilities.

The ACSC supported the Australian Government and key industry organisations, including the health sector, to reduce the risk of malicious cyber activity against the COVID-19 vaccine rollout. This included providing technical advice and assistance (including sector specific advice and assistance), earlier cooperation with vaccine supply chain entities, threat intelligence sharing, and vulnerability scanning of research, health, biotechnology, logistics and transport sectors.

The ACSC provided cyber security advice and support to the delivery of national systems for the management of COVID-19, including the Eligibility Checker, the Service Finder, the Symptom Checker, the Register Your Interest platform and the National Booking System.

What does the future hold?

The coronavirus pandemic demonstrated the ways in which malicious cyber actors can take advantage of national and global crises to conduct a range of activities, from mass phishing campaigns through to targeted attacks against vulnerable entities – particularly those entities charged with responding to a crisis. As new crises emerge, malicious cyber actors will attempt to employ the same techniques against Australia, manipulating uncertainty to their advantage and relying on common security lapses to maximise their chances of success.

ACSC Initiative: Collaboration with Telstra and Services Australia to combat malicious COVID-19 themed phishing

On 15 September 2020, the then Minister for Defence announced that the ACSC, in collaboration with Telstra and Services Australia, had launched a pilot program to identify and reject illegitimate phishing text messages that impersonate myGov and Centrelink before they reached Telstra customers. The ACSC continues to work with the broader telecommunications industry towards an industry-wide solution, and strongly encourages all organisations and individuals to exercise caution and remain vigilant when clicking links.

Any account can be compromised and malicious links can be sent from email accounts, messaging applications and SMS.

ACSC Initiative: Successful takedown notifications – COVID-19

On 25 January 2021, an Australian government department reported an ongoing SMS phishing campaign targeting members of the public. The campaign employed a website link in the SMS message to direct recipients to a credential and PII-harvesting page that impersonated the department. The ACSC assisted the department in taking the page down. This incident highlights the ongoing exploitation by malicious actors to leverage local and global events, including of the coronavirus pandemic, to increase the likelihood of individuals clicking malicious links.

The ACSC has enhanced its capability to respond at speed and scale to websites hosting malicious content. Since the commencement of the current takedown service in March 2021, the ACSC has removed more than 7,700 websites or services from the internet that were hosting malicious content related to the coronavirus pandemic. This is a significant increase compared to the same period in 2020. During this period, the ACSC was primarily focused on protecting the national vaccine supply, which resulted in more than 58 per cent of removals occurring within 24 hours of identification. During this period, 96.9 per cent of malicious web services detected were taken down.

Case Study: Ransomware attacks disrupt critical Australian health services

On 16 March 2021, the ACSC was informed of a ransomware incident affecting one of Melbourne's larger metropolitan public health services. Some of the health service's servers and workstations were infected with a Ryuk ransomware variant. This resulted in a partial IT system shutdown in the health service and the postponement of some elective surgeries.

The incident was detected by an unauthorised change to group policies. Indicators of compromise led the health service ICT team to promptly cut internet connectivity and enact incident response. The Digital Health Incident Management Team at the Department of Health, Victoria, was promptly contacted by the health service and a coordinated cyber incident response commenced, engaging incident response resources within the Department, contracted incident response partners, Victorian government agencies and the ACSC.

Prompt actions by the health service, the use of the advanced cybersecurity tools provided by the Department, and collaboration between the health service, government and contracted cyber security partners significantly reduced the impact of the ransomware attack and the restoration time.

The health service reported that the attack did not compromise patient safety. However, the attack disrupted the delivery of critical health services for hospitals. The four hospitals run by the health service provide a range of emergency, surgical, medical and general healthcare services. These include maternity, palliative care, mental health, drug and alcohol, residential care, community health and state-wide specialist services.

The health service implemented its business continuity plan. Offline backups were available. These were not affected by the ransomware attack, which helped to recover full capacity for patient care, even while IT systems were still impacted by the cyber incident.

This incident demonstrates the continued targeting of the health sector by cybercriminals during the pandemic, and shows the need for organisations to have incident response plans in place and to make regular offline backups to increase their resilience in the event of a cyber security incident.

How to protect networks

Spot COVID-19 themed malicious cyber activity

Identify COVID-19 related scams, online fraud attempts and phishing emails by stopping and thinking:

- Authority: Does the message claim to be from someone official?
- Urgency: Is there a limited time to respond?
- Emotion: Does the message evoke panic, fear, hope or curiosity?
- Scarcity: Is the message offering something in short supply?

Check if a COVID-19 message is legitimate:

- Go back to trustworthy sources. Visit the official website, log into an account, or phone the officially advertised phone number. Don't use the links or contact details in the message received.
- Check to see if the official source has stated they will never ask for certain details.

Protect remote working environments

Individuals and Australian organisations continue to be targeted by malicious actors with COVID-19 related scams, online fraud attempts and phishing emails. Consider the following steps to protect a remote working environment:

- Be aware of scams – educate employees to recognise scams and social engineering and the risks associated with phishing, including opening malicious links and using social media networks. Raise awareness of good personal cyber security hygiene.
- Enable multi-factor authentication – have multi-factor authentication enabled by default on any corporate networks, devices or systems.
- Update devices and systems – update software and turn on automatic operating system updates.
- Use passphrases – these are most effective when they are long, complex, unpredictable and unique.
- Follow the ACSC's COVID-19 specific guidance for: individuals working from home, small and medium businesses, large organisations (Operational Technology Environments), and government.
- Use a virtual private network (VPN) – these are an additional layer to securing web browsing and remote access over Wi-Fi. Note that this does not secure actual devices or online accounts, so it is important that these are also up to date.

Stay updated

The ACSC has released the following updates about COVID19 malicious cyber activity:

- COVID-19 themed malicious cyber activity
- COVID-19 malicious scams - threat awareness and guidance

ACSC Australian Cyber Security Centre

Ransomware

** Malicious cyber activity varies; the diagram below is one example of how cyber actors conduct ransomware attacks against devices and systems.*

Cyber actors can compromise and encrypt sensitive files on IT systems, threatening to release, block access to, or delete the files unless a payment is made.

Precursor malware is often deployed through phishing emails, remote access, or by exploiting vulnerabilities in applications or software. The malware is then used to deploy ransomware.

Once the cyber actor has access to the victim's systems, files may be exfiltrated and encrypted.

A ransom demand is made, indicating the amount to be paid (almost always in the form of untraceable cryptocurrency such as Bitcoin) and deadline. The actor may use other tactics in an attempt to further extort victims who do not pay.

If a victim pays the ransom, the cyber actor may provide a decryption key to allow the victim to unlock the files. The actor may separately demand a ransom to prevent release of stolen data.

The ACSC does not recommend payment of ransom demands. Paying ransom demands does not guarantee that files will be unlocked, and may increase the risk of being retargeted in future.

*Note the ACSC is aware of cases where payment was made, but the decryption process took longer than other recovery options available.

Ransomware cybercrime reports increased by

15%

Nearly 500 ransomware cybercrime reports received

Average of more than one ransomware cybercrime report received every day

Ransomware

Consistent with global trends, ransomware remains one of the most disruptive threats to Australian organisations. Ransomware can cripple organisations that rely on computer systems to function by encrypting devices, folders and files and rendering systems inaccessible. At the same time, cybercriminals have moved towards stealing data, including intellectual property and the personal information of employees and customers. The criminals then demand payment in return for decrypting and restoring access to the victim's network, and not publicly releasing the stolen information.

While all Australian organisations should remain alert to the threat of ransomware, top-tier cybercriminals have demonstrated a growing preference for using ransomware to hunt 'big game' entities – those they perceive as high profile, high value, and/or those that provide critical services. The preference for big game hunting means that ransomware attacks may have rapid and serious consequences for the Australian community if deployed against essential services or critical infrastructure (see case studies on pages 28, 33 and 34).

The increasing trend of data theft, encryption and public shaming reflects the ongoing evolution of ransomware tactics designed to ensure its financial success. The combination of encryption and data theft is known as 'double extortion'. Organisations who have previously been well-prepared for, or able to recover from, encryption alone are unlikely to be immune to this tactic. Enormous payments have been requested, usually in cryptocurrency, in return for the promise of non-publication of sensitive data. This further demonstrates the value of personal or sensitive commercial information and the willingness of cybercriminals to exploit any opportunity for profit. Victims must now also evaluate the cost of ransom payment against the legal, commercial and reputational consequences of a data breach.

ACSC advice on payment of ransom demands

The ACSC advises against paying a ransom. Doing so does not guarantee a victim's files will be restored, nor does it prevent the publication of any stolen data, or it being sold for use in other crimes. Along with increasing the likelihood of a victim being targeted again, each ransom payment also bolsters the viability of the ransomware market and puts other Australian organisations at greater risk.

Irrespective of the decision to pay a ransom, all victims are strongly encouraged to report ransomware-related cybercrime and cyber security incidents to the ACSC. Sharing technical and contextual information about an incident helps to protect other potential victims, supports efforts to disrupt criminal operations and enables the ACSC to implement measures to reduce ransomware targeting against Australia.

New business models make ransomware available to a broader range of offenders, akin to a criminal franchising arrangement. During the 2020–21 financial year, the ACSC observed an increase in professional syndicates operating ransomware-as-a-service (RaaS), which enables affiliates to use predeveloped ransomware tools to execute ransomware attacks in return for providing a percentage of the profits to the syndicate. This development has contributed to an increase in ransomware globally and enabled the targeting of a wider range of victims.

The ACSC operates in collaboration with domestic and international intelligence and law enforcement partners to:

- address the global threat of ransomware through collaboration and information sharing, to disrupt the syndicates causing greatest harm
- prevent and disrupt cybercrime by providing operational intelligence regarding offshore cybercriminals targeting Australia, and
- prevent and mitigate ransomware attacks. For example, in April 2021, the ACSC prevented an Australia-based financial company from becoming the victim of the Ryuk variant of ransomware. By analysing information from previous ransomware incidents, the ACSC identified potential victims and provided technical advice to mitigate the threat of ransomware attacks.

To support Australians in avoiding and recovering from ransomware incidents such as the above, the ACSC provides technical advice and guidance to the public on active ransomware software via cyber.gov.au. In December 2020, the ACSC launched the *Act Now, Stay Secure* media campaign, the first phase of which focused on providing advice to Australians on protecting themselves from ransomware.

The campaign promoted new technical ransomware guides, published by ASD and available on cyber.gov.au, including a prevention and detection guide, an emergency response guide and two step-by-step guides. In addition to the *Act Now, Stay Secure* campaign, ASD provided advice on a range of other mitigation methods, including an updated Essential Eight Maturity Model, threat level services, and the Partner Portal that informs the public of Australia's current cyber threat levels.

ACSC Initiative: Critical Infrastructure – Uplift Program (CI-UP)

The ACSC has launched CI-UP to help protect Australia's essential services from cyber threats by raising the security levels of critical infrastructure organisations. CI-UP is part of the Australian Government's Cyber Enhanced Situational Awareness and Response (CESAR) package and complements the Government's ongoing work to protect critical infrastructure security through proposed amendments to the *Security of Critical Infrastructure Act 2018*.

CI-UP will build knowledge and expertise for critical infrastructure providers to strengthen their cyber defences. CI-UP has been designed to:

- evaluate the cyber security maturity of critical infrastructure and systems of national significance using the Cybersecurity Capability Maturity Model (C2M2)
- deliver a set of prioritised vulnerability and risk mitigation recommendations to partners and assist them to plan for, and implement, these recommendations based on risk
- connect partners to other ACSC services.

Further information on CI-UP, including how to register to participate in the pilot, is on the ACSC website at: Critical Infrastructure Uplift Program (CI-UP).

Case Study: Ransomware attack disrupts Australian university

In February 2021, an Australian university's technology environment was compromised as a result of a targeted ransomware cyber attack infiltrating the university's infrastructure and applications. This led to the unprecedented decision by the university to shut down the network, ensuring the potential for further propagation was contained and critical learning and teaching could continue as scheduled.

Following identification of the infiltration, the focus was on containment, investigation and core remediation and recovery. The university advised the ACSC that, based on independently verified analysis, there was no evidence to suggest any data breach had occurred.

This incident highlights that compromising systems with malware can significantly disrupt an organisation's services. The ACSC is aware that malicious cyber actors have used education sector networks to pivot to other networks, such as other universities, research centres and government agencies. Once on a network, cyber actors can easily exploit trusted relationships by using compromised accounts to spear phish individuals from other organisations of interest and maximise the spread of ransomware or gain access to sensitive information, such as intellectual property.

Case Study: Largest fuel pipeline in the US shut down by a cyber attack

On 7 May 2021, the administrative network of US fuel pipeline operator Colonial Pipeline was encrypted by an affiliate of the Darkside ransomware syndicate. The attack resulted in the company proactively shutting down its operations to contain the ransomware. While Colonial was able to manually restart sections of its pipeline in under 48 hours and was fully operational in six days, the shutdown had a substantial impact on the daily lives of many US communities along the east coast. Panic buying led to fuel shortages, and as a result, multiple US states declared a state of emergency and fuel prices rose considerably in the states most affected by the shutdown.

Following the shutdown, the Darkside syndicate published an online statement describing itself as 'apolitical,' and emphasising its actions were financially motivated and not aimed at 'creating problems for society.'

Colonial Pipeline later confirmed it had paid approximately $4.4 million (USD) ransom in bitcoin on the same day of the incident. Despite this, full automatic operations were not restored until six days later, with the media reporting that Darkside's decryption tool had not been sufficient to completely restore Colonial Pipeline's systems. Darkside subsequently claimed it had ceased its operations, citing law enforcement action as the reason for shutting down. The US Department of Justice later recovered about $2.3 million (USD) in bitcoin that the company had paid to the ransomware group.

The Colonial Pipeline compromise highlights the potential for malicious cybercriminal activity to cause widespread disruption to businesses and individuals, even when the actor has not aimed to disrupt critical infrastructure. It also demonstrates the challenges of fully recovering from a ransomware incident and that business operations can remain disrupted even when a ransom payment is made and decryption tools are provided. This underscores the importance of maintaining strong cyber security practices, as well as the value of critical infrastructure organisations engaging closely with the international cyber security centres, including the ACSC, during any incident.

Case Study: Global meat and food processing company shut down by a cyber attack

On 30 May 2021, JBS Foods, a global meat and food processing company, was compromised by the Sodinokibi/Revil ransomware syndicate. The incident led the company to proactively cease operations and stand down workers across facilities – including in Australia – while it investigated.

On 9 June 2021, JBS USA confirmed it paid the equivalent of $11 million (USD) in ransom to mitigate any unforeseen issues related to the attack and to provide assurance of no further disruption and to limit the potential impacts.

This incident, along with other high profile ransomware incidents in the 2020–21 financial year against US critical infrastructure and the health sector in the UK and Ireland, highlights cybercriminals' willingness to cause serious disruption – including financial, reputational and societal harm – for financial gain. Cybercriminals are specifically targeting entities whose services or data make them particularly vulnerable to extortion.

However, this incident also highlights the benefits to victim organisations and other potential victims of close collaboration with the ACSC. At the time of the incident, the ACSC engaged with JBS Australia, their independent incident response provider and international cyber security partners, to provide technical advice and assistance, including remediation advice and confirmation of the ransomware variant. This close cooperation assisted JBS Australia to rapidly respond to the incident and quickly restore operational systems from backups. The ACSC subsequently was able to identify indicators of compromise associated with the ransomware activity and protect other potential victims across Australia from compromise.

How to protect networks

Organisations can protect themselves from ransomware using the ACSC's tailored guidance below.

Individuals, and small and medium-sized businesses

Follow the steps in the ACSC's Ransomware Prevention and Protection Guide:

- Update devices and systems – update software and turn on automatic operating system updates
- Enable multi-factor authentication – have multi-factor authentication enabled by default on any corporate networks, devices or systems
- Backup data – set up and perform regular offline backups; these are essential for recovery following a ransomware attack. Backups must be stored offline or otherwise isolated from the corporate network
- Implement access controls – restrict administrator privileges and do not share or re-use login details
- Turn on ransomware protection – available on some operating systems.

Prepare a Cyber Security Emergency Plan – prepare and regularly exercise this plan to ensure everyone is familiar with the processes and understands their roles.

Government, large organisations and infrastructure

Implement the ACSC's Essential Eight Mitigation Strategies and Strategies to Mitigate Cyber Security Incidents.

For further information and advice on ransomware, including prevention and mitigation, visit:

- Ransomware in Australia
- Ransomware targeting Australian aged care and health sectors
- Mitigating malware and ransomware attacks - The United Kingdom's National Cyber Security Centre (NCSC)
- Ransomware guidance and resources - The United States Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA)

ACSC Australian Cyber Security Centre

Exploitation of security vulnerabilities

** Malicious cyber activity varies; the diagram below is one example of how cyber actors can exploit vulnerabilities and gain access to devices and systems. As patching vulnerable software or devices may not always remove a malicious actor from an already compromised network or system, further investigation may be required to identify malicious activity.*

A security vulnerability within a device or software application is discovered and publicly reported.

Note: Exploit code may already be in use by some actors taking advantage of the vulnerability prior to the public announcement.

The vendor usually releases an update or patch to resolve the vulnerability, encouraging users to implement the patch on systems, devices or software.

Cyber actors create exploits to target security vulnerabilities in unpatched systems, devices or software.

The cyber actor may directly target vulnerable servers to access systems.

Exploits may also be delivered via:

- attachments to email messages
- compromised websites
- social networking sites

Exploits may drop malware onto vulnerable systems OR allow cyber actors remote access into a network.

Unsuspecting users are lured into executing the exploit through social engineering techniques.

Exploitation of security vulnerabilities

Throughout this period, the ACSC has observed a continuing trend of state-sponsored actors and cybercriminals rapidly exploiting publicly reported security vulnerabilities to compromise large numbers of organisations. Malicious cyber actors monitored public reporting of vulnerabilities and used vulnerability scanning tools against internet-accessible networks to identify unpatched software and hardware appliances, as well as misconfigured devices and networks, for exploitation. Security vulnerabilities were sometimes exploited within hours of a patch release or technical write up – particularly if proof of concept (PoC) code was also available.

While improving cyber hygiene and rapid patching can help protect organisations from being compromised via publicly reported security vulnerabilities, zero-day exploits are more difficult for organisations to defend their networks against. This is because a zero-day is a software exploit that has not been disclosed or patched by the software vendor.

Both zero-day exploits and exploits of publicly reported security vulnerabilities can have significant impacts. For example, the 2021 'ProxyLogon' Microsoft Exchange server vulnerabilities exploit was wide-scale and will have long lasting impacts for many vulnerable organisations that did not patch and remediate their systems in time. Similarly, malicious actors rapidly exploited 2020 mobile device management vulnerabilities, and a range of organisations were extorted after their data was stolen via compromised Accellion FTAs (see Case Study: Accellion FTA compromises Australian organisations and state government agencies, page 39).

The ACSC assesses that exploitation of publicly reported vulnerabilities will continue to be a key vector used by malicious cyber actors into the future. The exploitation of such vulnerabilities is scalable, low cost and avoids the need to develop zero-day exploits. These exploits are not, and will not be, limited to the targeting of government entities and large organisations. The ACSC and national security partners have observed exploits for a number of publicly reported vulnerabilities being deployed across the full span of Australian networks, including private industry, small businesses and home users.

ACSC Initiative: Cyber Hygiene Improvement Programs (CHIPs)

The ACSC's Cyber Hygiene Improvement Programs (CHIPs) involve a series of cyber hygiene campaigns to improve the cyber security posture of Commonwealth, state, territory and local government entities. CHIPs also conduct high-priority operational tasking activities in response to identified and potential cyber threats or significant events.

Through these activities, CHIPs can quickly build visibility of, and develop insights into, security vulnerabilities across Commonwealth, state, territory, and local governments, and guide urgent remediation work. In the 2020–21 financial year, 34 high-priority operational tasking activities were undertaken. This included scans of:

- the remote access and working-from-home arrangements implemented by Commonwealth entities in response to the coronavirus pandemic
- all Australian-attributed IP addresses to identify compromised on-premises Microsoft Exchange servers and Microsoft Windows Domain Controller Zerologon vulnerabilities (see Case Study: Widespread compromises via Microsoft Exchange server vulnerabilities, page 38)
- all Commonwealth entities in response to the release of a mobile device management PoC exploit code.

Case Study: Widespread compromises via Microsoft Exchange server vulnerabilities

On 3 March 2021, Microsoft announced that it had detected multiple actors using zero-day vulnerabilities to compromise on-premises Microsoft Exchange servers in limited and targeted attacks. Microsoft issued a patch to assist vulnerable organisations; however, this would not remove any malicious actors already present on victim networks before the patch was applied. Following Microsoft's patching advice, the ACSC observed malicious actors rapidly exploiting these vulnerabilities in unpatched Microsoft Exchange servers.

The vulnerabilities in Microsoft Exchange servers effectively meant a malicious actor could access emails and other information or content stored on, or accessible by, that server. Once an actor exploited the vulnerability they could access email communications, take data and move further into a network. If organisations did not look for indicators of compromise, the vulnerability could lead to identity theft, unauthorised access to personal accounts and unlawful exfiltration of data, with the risk of extortion.

On 19 July 2021, the Australian Government released a joint statement by the Australian Foreign Minister, Minister for Defence and Minister for Home Affairs joining international partners in expressing serious concerns about malicious cyber activities by China's Ministry of State Security (MSS), and the Australian Government's determination that China's MSS exploited vulnerabilities in the Microsoft Exchange software affected thousands of computers and networks worldwide, including in Australia.

Since 3 March 2021, the ACSC has worked closely with government and industry partners to identify vulnerable organisations and offer remediation advice. The ACSC published an alert on its website on 3 March 2021, updated several times since, and a technical advisory on 12 March 2021. The ACSC supported Microsoft in identifying and assisting vulnerable customers by using the ACSC's CHIPs scanning activities.

The Microsoft Exchange server experience – both in Australia and globally – reinforces the importance of remaining aware of the cyber security threat environment, and following ACSC advice.

Case Study: Accellion FTA compromises organisations and state government agencies

In January 2021, the ACSC became aware of cyber actors exploiting vulnerabilities in the legacy Accellion FTA used by a range of organisations. The Accellion FTA is a software that allows for the sharing of files between users; and actors exploiting a vulnerability in the legacy software were able to gain access to content stored on, and accessible by, the organisation's FTA instance. This activity impacted organisations globally, including Australian organisations, many of which have since retired FTA and migrated to Accellion's modern content firewall Kiteworks platform, consistent with ACSC and international partners' advice.

On 19 January 2021, the ACSC published an alert, as well as an advisory to ACSC Partners, providing technical advice and mitigation measures to address the vulnerability in the FTA. The ACSC also engaged with a number of Australian organisations identified as users of the Accellion FTA and recommended they investigate their security posture. On 1 March 2021, Accellion announced all FTA vulnerabilities remediated and an end-of-life for its FTA product, effective 30 April 2021. In addition, Accellion offered its FTA customers free forensic assistance, as well as an independent forensic analysis by Mandiant, access to Accellion senior management, migration services to Kiteworks, or migration assistance to customers who elected to terminate their relationship with Accellion.

ACSC investigations identified several organisations that were affected by the Accellion compromise, including in the energy, professional and legal services and health sectors, as well as a number of NSW government agencies.

On 23 February 2021, the NSW Government publicly released a statement advising that it had established Strike Force Martine to investigate the impacts of the breach on the NSW Government. Transport for NSW and NSW Health are among the agencies that were affected by the incident. Transport for NSW has confirmed there was no third party access to major agency systems including drivers licence systems or the Opal Travel systems. NSW Health has confirmed that medical records in public hospitals were not affected and the software involved is no longer in use by NSW Health.

Consistent with ACSC advice, the NSW Government retired all instances of the Accellion FTA as part of the centralised response to protect customer and government data. The ACSC worked closely with Cyber Security NSW to understand the impact of the breach, including to customer data.

The global Accellion FTA compromise demonstrates the importance of vendors regularly assessing security vulnerabilities and ensuring prompt notification if any are found, including those posed by third-party service providers that may be using legacy products.

The ACSC recommends that organisations mitigate the risk exposure posed by legacy third party products. Cyber actors continue to rapidly leverage publicly reported vulnerabilities in legacy products to target unpatched systems and devices. Agencies running legacy or unsupported software are encouraged to review their risks, implement timely patches, upgrade to newer, supported software, and have an incident response plan in place.

How to protect networks

Individuals, and small and medium-sized businesses

- Update devices and systems – update software and turn on automatic operating system updates.
- Have a cyber incident response plan in place and apply appropriate cyber security measures proportionate to the risk of compromise.

Government, large organisations and infrastructure

Know the networks and the security risks:

- The ACSC encourages all users to review their networks to establish where their most valuable and sensitive information lies, and understand their risks.
- Have a cyber incident response plan in place and apply appropriate cyber security measures proportionate to the risk of compromise.

Prioritise patching within 48 hours of a patch release:

- Adversaries use automated tools to regularly scan for and exploit network vulnerabilities, often within 24 to 48 hours of public reporting of a vulnerability.
- This means that where an exploit exists, organisations should prioritise patching within 48 hours of a patch release to protect their networks from malicious activity.

Follow ACSC advice:

- System patching
- Implement network segmentation and segregation
- Operating system hardening
- Web shell malware
- Web Shells – Threat Awareness and Guidance

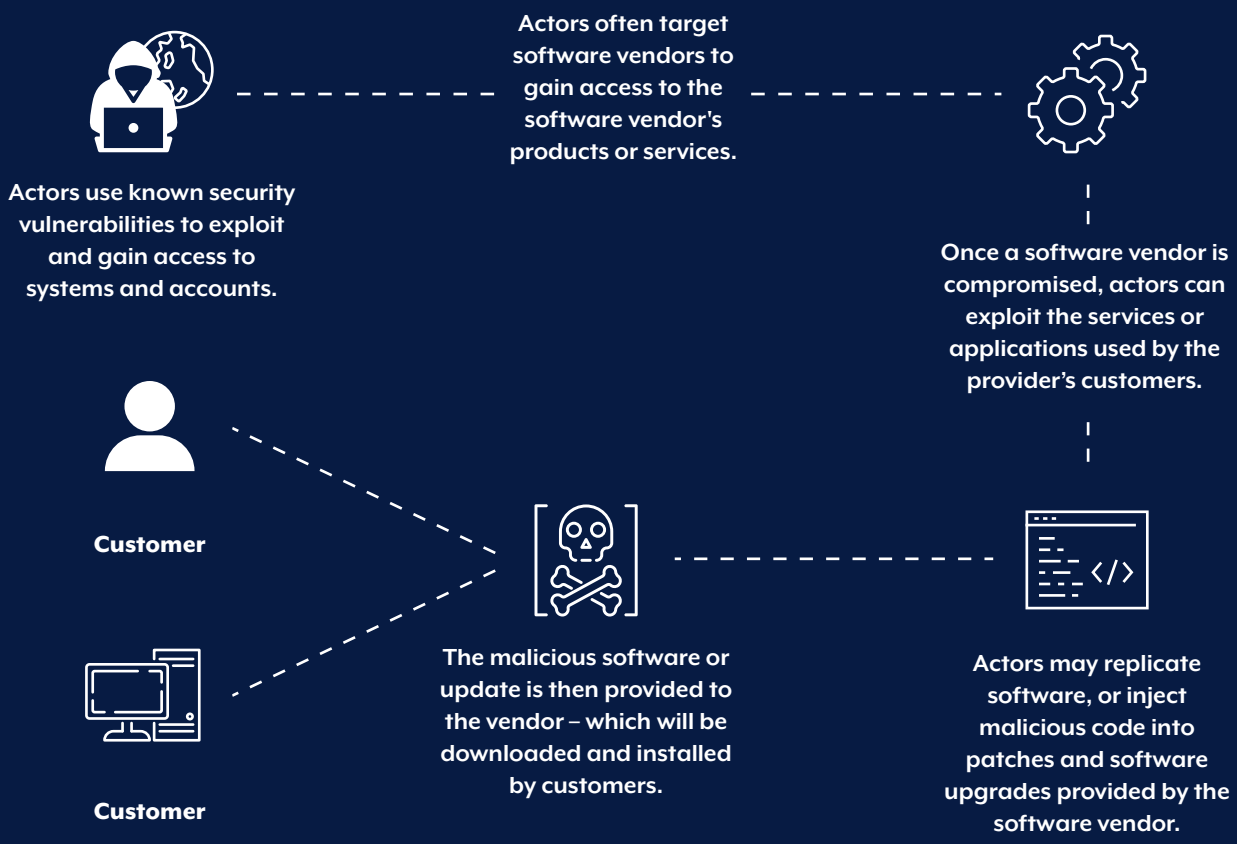
Stay updated

The ACSC regularly updates advice on known vulnerabilities as well as the detection, prevention and mitigation of malicious activity:

- ACSC Alerts
- ACSC Advisories
- Advisory 2021–002: Active exploitation of Microsoft Exchange servers

Software supply chain compromises

**Malicious cyber activity varies; the diagram below is one example of how cyber actors can exploit cyber supply chains to gain access to devices and systems.*



Software supply chain compromises

In the 2020–21 financial year, the ACSC observed software supply chain compromises where a malicious cyber actor accesses a vendor's network and covertly modifies its software. Software exploitation can occur at any point in the software development lifecycle, from the design, distribution and support phases – including via the release of patches and updates – through to the decommissioning phase. After the modified software is released, the actor uses it to access the networks of the vendor's customers and to conduct follow-on malicious activities.

While software supply chain compromises can be difficult to detect and defend against, there are measures that can minimise their impact. These include assessing the risks a vendor introduces to networks and reviewing internal and external network security vulnerabilities to prevent third party access to systems. Once detected, mitigation can be particularly challenging, as the malicious actor has often been able to develop pervasive access to a range of victims over an extended period of time. The ACSC recommends organisations plan for incident response in the event of a software supply chain compromise.

Supply chain compromises present a high-impact cyber threat that will only increase as networks continue to incorporate more third-party software. Supply chain compromises will largely remain within the purview of advanced state-sponsored actors and likely concentrate on high-value targets that are not as susceptible to simpler methods of compromise. However, skilled cybercriminals may also increasingly focus their efforts on supply chain exploitation as a means of compromising many victims at scale.

Case Study: Multiple global victims following Russia's SolarWinds Orion software compromise

In December 2020, Mandiant publicly announced a 'highly skilled actor' was conducting a global intrusion campaign enabled by the compromise of the SolarWinds Orion platform software. SolarWinds is a US software firm which produces a wide range of IT infrastructure monitoring and management tools. The compromise meant that organisations running SolarWinds Orion platform software may have inadvertently installed malicious additions through normal update processes, and potentially provided actors with the ability to access users' systems.

The US Government issued a statement on 15 April 2021 attributing the SolarWinds Orion compromise to Russian state actors. The same day, the Australian Government released a joint statement by the Australian Foreign Minister, Minister for Defence and Minister for Home Affairs joining international partners in determining that Russian state actors were actively exploiting SolarWinds and its supply chains. Russia's campaign has affected thousands of computer systems worldwide.

Following detection of the compromise, SolarWinds acted quickly to release progressive advice from 14 December 2020 in order to assist organisations to remediate this vulnerability, including patches and guidance to support identification of vulnerable versions of the Orion platform. SolarWinds engagement with the ACSC through provision of international insights during this incident informed ACSC's understanding of the potential impact to Australian organisations and its advice to Australians. The ACSC welcomes the positive collaboration with SolarWinds in order to share the lessons learned with other supply chain providers and organisations. This ensures the protection of their software and networks from similar occurrences and enhances Australia's overall cyber security resilience.

How to protect the cyber supply chain

Small and medium-sized businesses, large organisations and infrastructure, government

A robust and layered security approach is the best option for reducing the potential impact of this type of compromise, and increasing the chance of early detection. However, software supply chain compromises are particularly difficult to fully prevent due to their sophisticated and covert nature.

Identify and manage supply chain risks using the following:

- Cyber supply chain guidance
- Cyber supply chain risk management
- Identifying cyber supply chain risks
- Home Affairs: Critical Technology Supply Chain Principles

To enable early identification of malicious activity, and reduce cyber actors' ability to move laterally following a network compromise, apply the advice contained in the following documents:

- System patching
- Implement network segmentation and segregation
- Restrict privileged user accounts
- Web shell malware

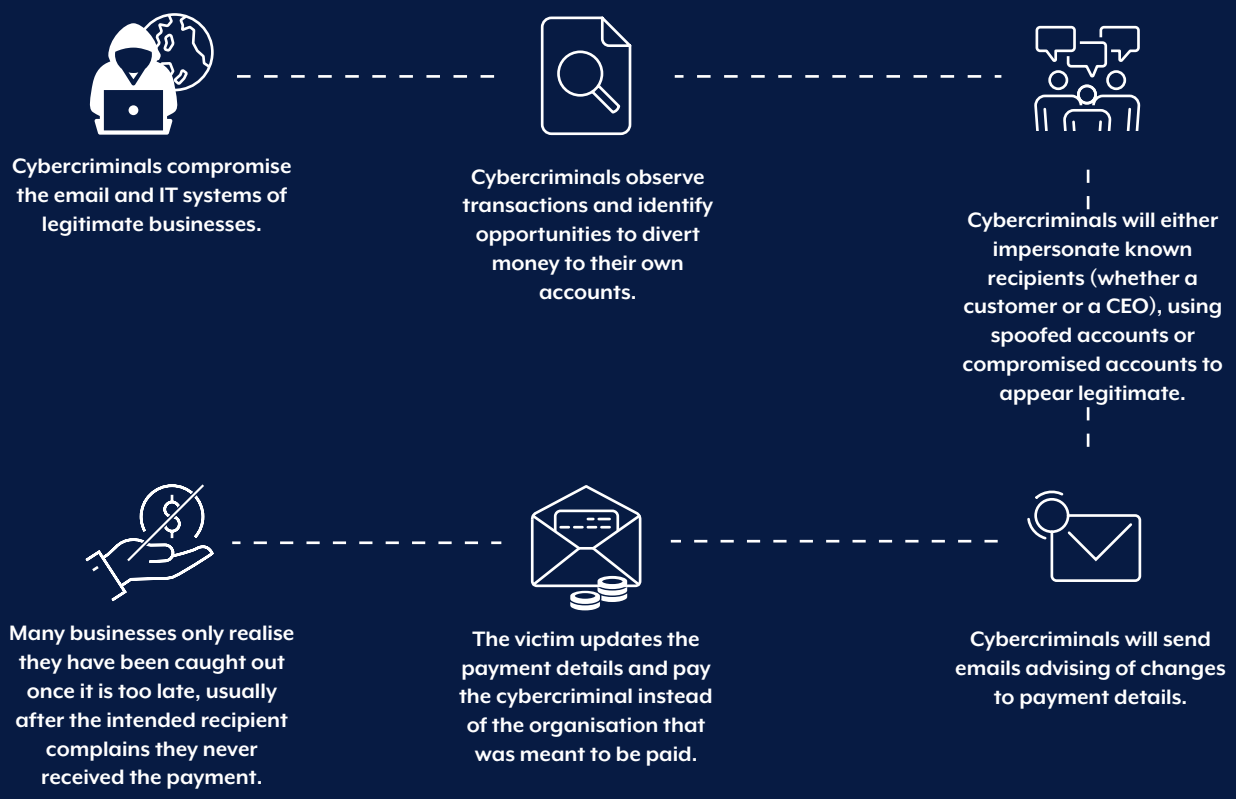
For further advice on mitigating cyber supply chain risks, visit:

- ACSC Alert: potential SolarWinds Orion compromise
- Mitigating use of stolen credentials
- Secure administration
- Cloud security guidance

ACSC Australian Cyber Security Centre

Business Email Compromise

**Malicious cyber activity varies; the diagram below is one example of how cyber actors use BEC to scam victims.*



More than

4,600 BECs reported

Over

$81 million (AUD)

lost due to BEC

Increase in average financial losses per BEC report

▲54%

Business email compromise

BEC often involves cybercriminals compromising a business or personal email account and impersonating a trusted supplier or business representative to scam victims out of money or goods. Because BEC often appears legitimate and rarely relies on malicious links or attachments, these emails can often get past security and technical controls, such as anti-virus programs and spam filters.

During the pandemic, there has been an increase in BEC targeting organisations, especially where their employees work remotely. International reporting shows cybercriminals using BEC to target organisations purchasing personal protective equipment or other supplies needed to combat the coronavirus.

BEC scams are sophisticated, insidious and growing as a threat to Australian organisations. Cybercriminal groups conducting BEC have likely become more organised, and have developed enhanced and streamlined methodologies which allow them to bypass victims' cybersecurity protocols, conduct reconnaissance and monitor email traffic to determine the most lucrative time to launch the scam. This not only increases the certainty of success but also increases the overall profit margin associated with the activity.

AFP Initiative: Operation Dolos, multi-agency BEC Taskforce

In response to the BEC threat, the BEC Taskforce was established to provide a coordinated effort to help prevent and investigate BEC. The taskforce comprises the AFP and all state and territory policing partners. In some BEC cases, the taskforce is able to recover funds that have been sent to overseas bank accounts. In the 2020–21 financial year, the AFP, through the multi-agency Operation Dolos – Business Email Compromise Taskforce, prevented more than $8.45 million (AUD) being lost from the Australian community to BEC.

Case Study: Australian hedge fund subject to BEC and declared bankruptcy

In September 2020, an Australian hedge fund was subject to BEC and forced to declare bankruptcy as a result. The BEC involved false invoices with the company transferring $8.7 million (AUD) to bank accounts controlled by the offenders. While the business recovered the majority of its funds, it suffered significant reputational damage and its main client withdrew. This forced the hedge fund to go into receivership and resulted in its bankruptcy. This was likely Australia's first bankruptcy case as a direct result of a cybercrime incident.

How to protect email from fraud and compromise

The success of BEC scams rely on a lack of training and awareness among employees. The most effective way to mitigate the threat of BEC is to educate staff on the following points:

- Verify payment-related requests – if staff receive a request to make a large transfer or to change bank account details, they should verify that the request is legitimate before actioning it. Call the sender's established phone number or visit them face-to-face before transferring any funds.
- Identify fraudulent emails – ensure staff are trained to recognise suspicious emails, including fraudulent bank account change or requests to check or confirm login details. The latter may be a phishing attack which could compromise account security.

While the implementation of technical controls is less important in preventing BEC, there are still a number of measures organisations and individuals can undertake to secure their email communication, including:

- Enable multi-factor authentication – have multi-factor authentication enabled on all email accounts to help prevent unauthorised access.
- Implement email authentication measures – email authentication protocols such as SPF, DKIM, and DMARC can help prevent email spoofing attacks.
- Secure email gateways and servers – protect your organisation with measures such as email content filtering.

For more detailed advice on BEC including prevention and mitigation measures, visit:

- Protecting against BEC
- Protect your business from email fraud and compromise
- Malicious email mitigation strategies
- Cyber security awareness training

How to prepare for, protect against and respond to cyber security incidents

How to prepare for, protect against and respond to cyber security incidents

Be aware of the cyber threat environment

Stay across ACSC advice

The ACSC provides critical and timely advice concerning cyber security incidents as they happen. Stay across ACSC advice by subscribing to the ACSC alert service to receive tips and techniques to help protect internet users at home, at work and on mobile devices. You can also follow the ACSC on Twitter, Facebook and LinkedIn to stay up-to-date on the latest cyber threats and advice.

The cyber.gov.au website is the one-stop-shop for access to ACSC services including advice and guidance products, online instructional self-help materials, and ReportCyber, and to sign up for the ACSC partnership programs and alert service. The website provides advice and information to individuals, families, small-to-medium businesses and large-scale organisations and government.

Become an ACSC Partner

The ACSC Partnership Program facilitates ACSC engagement with Australian organisations and individuals to lift cyber resilience across the Australian economy. The ACSC Partnership Program comprises three tiers:

Network Partners

For organisations with cyber security professionals across governments, critical infrastructure, industry, academia and the research sector. ACSC Network Partners are provided access to threat intelligence, advisories and advice to enhance situational awareness, as well as collaboration opportunities with fellow cyber security professionals, resilience-building activities (e.g. exercises, discussions, workshops), and the Joint Cyber Security Centre (JCSC) network.

Business Partners

For businesses that would like to be kept up-to-date with relevant cyber security information for their businesses. Business partners are provided with advice to gain a better understanding of the cyber security landscape, including the steps required to protect themselves from cyber security threats.

Home Partners

For individuals and families that would like to be kept up-to-date with relevant information. Home Partners receive advice that provides them with a better baseline understanding of the cyber security environment.

Sign up to the ACSC Partnership Program by visiting the Partner Hub and filling in a form.

Joint Cyber Security Centres

The JCSCs in Sydney, Melbourne, Brisbane, Adelaide, and Perth, along with virtual JCSCs in Darwin and Hobart, provide opportunities for ACSC Network Partners in the Australian cyber security community to come together in a trusted, neutral environment. The JCSCs amplify the cyber security efforts of the ACSC by engaging with Network Partners in government, industry, academia and the research community. The JCSCs host a regular series of workshops and events for Network Partners, and provide collaborative workspaces to address common challenges within and across sectors.

The Australian Government has invested in expanding support to small to medium businesses and individuals through cyber.gov.au and the placement of Home Affairs Outreach Officers in each JCSC.

If you are interested in becoming an ACSC partner and accessing the JCSC services, visit the ACSC website.

Uplift cyber security

ACSC's cyber security mitigation strategies

The ACSC has produced a range of guidance covering all cyber security maturity levels, including government, large organisations, small to medium businesses and individuals. Implementing this guidance makes it much harder for malicious cyber actors to compromise systems and helps all Australians to stay secure online.

Flagship cyber security advice for Australian organisations

While no set of mitigation strategies are guaranteed to protect against all cyber threats, organisations are recommended to implement eight essential mitigation strategies from the ACSC's Strategies to Mitigate Cyber Security Incidents as a baseline. This baseline, known as the Essential Eight, makes it much harder for malicious cyber actors to compromise systems. Furthermore, proactively implementing these strategies can be more cost-effective in terms of time, money and effort than having to respond to a large-scale cyber security incident.

The Essential Eight Maturity Model, first published in June 2017 and updated regularly, supports the implementation of the Essential Eight. It is based on the ACSC's experience in producing cyber threat intelligence, responding to cyber security incidents, conducting penetration testing and assisting organisations to implement the Essential Eight.

Further information on the Essential Eight is on the ACSC website at: Essential Eight

Tailored advice for small and medium businesses, individuals and families

The ACSC has a number of publications tailored to small and medium businesses, and individuals and families. This guidance can be found on the small and medium businesses and individuals and families sections of cyber.gov.au, and the key publications below.

The Small Business Cyber Security Guide has been specifically designed for small businesses to understand, take action and increase their cyber security resilience against ever-evolving cyber security threats. It includes simple mitigation strategies that have been derived from the Essential Eight and are written in clear language. Further information on cyber security for small businesses and these mitigation strategies can be found in the full Small Business Cyber Security Guide.

The ACSC also provides detailed information on how to prevent and respond to particular cyber security threats affecting small to medium businesses:

- To mitigate ransomware attacks, see the Ransomware Prevention and Protection Guide and the Ransomware Emergency Response Guide.
- To mitigate attacks on email, including email compromise or impersonation, see the Email Security Prevention and Protection Guide and the Email Security Emergency Response Guide.

For individuals, the ACSC provides guidance on Easy Steps to Secure Your Devices and Accounts – five key actions that people can take to protect themselves from large scale, low sophistication malicious cyber activity such as cybercrime.

Other mitigation resources on the ACSC's website include the Quick Wins series and Step-by-Step Guides. The Quick Wins series provides a brief overview of cyber security threats requiring mitigation, while the Step-by-Step Guides provide easy-to-follow instructions on how to enable basic cyber security measures such as multi-factor authentication.

Participate in ACSC programs and services

Cyber Threat Intelligence Sharing (CTIS) Platform

The ACSC's Cyber Threat Intelligence Sharing (CTIS) program is enhancing how partners share intelligence about malicious cyber activity with governments, critical infrastructure, industry and education partners in an automated fashion and at machine speed.

The CTIS program is co-designing with ACSC Network Partners enhancements to its CTIS platform and business rules to enable multi-directional sharing across collaborative communities. The ACSC is also developing integration with Malware Information Sharing Platform (MISP) users to increase interoperability. The program will also support the development of government and industry-led communities of practice and other methods of collaboration to more effectively share threat intelligence.

ACSC initiatives for Australian Government

The ACSC has developed and operates a set of capabilities that can further assist government entities in improving their cyber resilience, including, but not limited to:

- The Cyber Maturity Measurement Program (CMMP) undertakes cyber security measurements for Commonwealth entities against the Essential Eight Maturity Model.
- The ACSC Cyber Security Uplift Services for Government program takes recommendations from the CMMP and assists Commonwealth entities to improve their cyber security awareness and posture.
- The Cyber Security Aftercare Program (CSAP) is a program that ensures the ACSC stays in touch with Commonwealth entities, assisting them on their cyber security journey following incidents or uplift activities.
- The Cyber Toolbox is an umbrella term for a collection of in-house developed software tools and processes, designed to aid in elevating cyber security maturity for government entities.
- The Cyber Hygiene Improvement Programs (CHIPs) are a series of campaigns to that measure cyber security posture and hygiene across Commonwealth, state and territory governments, providing objective data to guide targeted management.

Be prepared for a cybercrime or cyber security incident and know how to respond

Have an incident response plan and arrangements

Organisations should prepare for a cyber security incident by having incident response, business continuity and disaster recovery plans in place, and testing them. A cyber incident response plan transparently outlines agreed organisational responses to a range of cyber security incidents (see the Cyber Incident Response Plan section below). Testing through cyber exercises in a controlled environment enables organisations to respond decisively and consistently to realworld cyber security incidents, limiting potential impacts and supporting organisational recovery.

Cyber Incident Response Plan

The ACSC has developed a Cyber Incident Response Plan Template and Cyber Incident Response Readiness Checklist, which is available to ACSC Partners on the Partner Portal. These documents are intended to be used as a starting point for Australia's critical infrastructure and essential services to develop their own Cyber Incident Response Plan and Cyber Incident Response Readiness Checklist.

While many cyber security incidents can be prevented or the impacts mitigated through good cyber security practices, such as implementation of the Essential Eight Maturity Model, risks will remain. Anyone can be the target, so it is essential that all organisations have a plan for responding to a cyber security incident.

Conduct cyber security exercises

A cyber security exercise is a controlled activity using a scenario in order to simulate a real-life cyber security incident. Regularly conducting cyber security exercises provides organisations with an opportunity to review plans, policies, capabilities, roles and responsibilities in a simulated and safe environment. As a result, cyber security exercises may prove invaluable in the development of an organisation's ability to respond to and recover from cyber security incidents.

Know how to report a cyber security incident or cybercrime

The ACSC website (cyber.gov.au) provides extensive advice, guidance and information on a range of cyber security matters.

Large organisations and critical infrastructure, government organisations, small and medium businesses and individuals can all report cyber security incidents through the ReportCyber website. The ACSC website also provides additional assistance and referral pathways depending on the nature of the incident or cybercrime.

The ACSC is contactable via email (asd.assist@defence.gov.au) or by calling the Australian Cyber Security Hotline on **1300 CYBER1 (1300 292 371).**