Australian Government
Australian Signals Directorate

ACSC
Australian
Cyber Security
Centre

July 2021 – June 2022

Annual Cyber Threat Report

About the ACSC

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

- the Australian Cyber Security Hotline, which is contactable 24 hours a day, 7 days a week, via 1300 CYBER1 (1300 292 371)
- publishing Alerts, technical advice, Advisories and notifications on significant cyber security threats
- cyber threat monitoring and intelligence sharing with our partners in Australia and overseas to counter cyber security threats
- Joint Cyber Security Centres (JCSCs) that support collaboration between over 80,000 Australian organisations and individuals on cyber security issues
- exercises and uplift activities to enhance the cyber security resilience of Australian organisations.

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

Foreword

I am pleased to present the third Annual Cyber Threat Report by the Australian Cyber Security Centre (ACSC), a key part of the Australian Signals Directorate (ASD).

Throughout its 75 year history, ASD has defended Australia from global threats and advanced our national interests. It remains at the frontline of defending our nation and keeping Australia safe and secure.

We are currently witnessing deteriorating strategic circumstances in our region and globally, including a military build-up unseen since World War II, and expanding cyber and grey zone capabilities are of particular concern.

In this environment, the work performed by ASD and its ACSC is more important than ever.

This expanded Annual Cyber Threat Report 2021–22 is the product of insights from across the Commonwealth, with the Australian Federal Police, the Australian Criminal Intelligence Commission, the Australian Security Intelligence Organisation, Defence Intelligence Organisation and the Department of Home Affairs also contributing to help all Australians better understand the cyber threat environment and improve their cyber defences.

Over the last financial year and reflecting strategic competition globally, we have all witnessed a heightened level of malicious cyber activity. Regrettably, too many Australians have also felt its impacts.

The government considers cyber security and reinforcing our online resilience to be a national priority. Increased investment in ASD's cyber and intelligence capabilities under project REDSPICE (Resilience, Effects, Defence, SPace, Intelligence, Cyber, Enablers) positions Australia to lift our defences and recognises the critical role ASD plays in our national security.

This report maps how threat actors across the world have continued to find innovative ways to deploy online attacks, with supply chains used to penetrate cyber defences of governments and organisations in many countries, including Australia.

The better news is that with increased collaboration across industry, small business, and government—and with all Australians—our joint cybersecurity future and the digital opportunities before us remain bright.

In many ways, this report is the product of all Australians with its foundations and findings formed by reports to the ACSC. Reporting cybercrime is vital for us to build a threat picture that can prevent others from falling victim to the ransomware syndicates and cybercriminals. The best cyber defence is informed by the best intelligence.

Together we can reach our ambitious goal to make Australia truly the most secure place to connect online. This report is another important step forward.

The Hon Richard Marles, MP

Deputy Prime Minister and Minister for Defence

Table of Contents

About the Contributors

Australian Signals Directorate

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.

ASD delivers intelligence, cyber security and offensive operations in support of the Australian Government and the Australian Defence Force.

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.

The ACIC contributes to the 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 enable the AFP to collaborate with other ACSC partners, triage new referrals, undertake targeted intelligence development and coordinate law enforcement responses to cybercrimes of national significance. The AFP also leads the Joint Policing Cybercrime Coordination Centre to harness the powers, experiences and investigative capabilities of Australian policing jurisdictions.

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, 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.

Defence Intelligence Organisation

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

Department of Home Affairs

The Department of Home Affairs leads cyber security policy for the Australian Government, including developing Australia's Cyber Security Strategy 2020 and overseeing its implementation.

Home Affairs Cyber and Infrastructure Security Outreach officers are co-located in the JCSCs. Outreach officers work with small and medium businesses, with a particular focus on critical infrastructure entities, or those entities that sit within the critical infrastructure supply chain, providing them with advice on where to access information to uplift their cyber security and resilience.

Executive Summary

Over the 2021–22 financial year, the deterioration of the global threat environment was reflected in cyberspace. This was most prominent in Russia's invasion of Ukraine, where destructive malware resulted in significant damage in Ukraine itself, but also caused collateral damage to European networks and increased the risk to networks worldwide.

In Australia, we also saw an increase in the number and sophistication of cyber threats, making crimes like extortion, espionage, and fraud easier to replicate at a greater scale. The ACSC received over 76,000 cybercrime reports, an increase of nearly 13 per cent from the previous financial year. This equates to one report every 7 minutes, compared to every 8 minutes last financial year.

The ACSC identified the following key cyber security trends in the 2021–22 financial year:

- **Cyberspace has become a battleground.** Cyber is increasingly the domain of warfare, as seen in Russia's use of malware designed to destroy data and prevent computers from booting in Ukraine. But Russia was not alone in its use of cyber operations to pursue strategic interests. In July 2021, the Australian Government publicly attributed exploitation of Microsoft Exchange vulnerabilities to China's Ministry of State Security. And a joint Five-Eyes Advisory in November 2021 confirmed exploitation of these vulnerabilities by an Iranian state actor. Regional dynamics in the Indo-Pacific are increasing the risk of crisis and cyber operations are likely to be used by states to challenge the sovereignty of others.
- **Australia's prosperity is attractive to cybercriminals.** According to a 2021 Credit Suisse report, Australia has the highest median wealth per adult in the world. In 2021–22, cybercrimes directed at individuals, such as online banking and shopping compromise, remained among the most common, while Business Email Compromise (BEC) trended towards targeting high value transactions like property settlements.
- **Ransomware remains the most destructive cybercrime.** Ransomware groups have further evolved their business model, seeking to maximise their impact by targeting the reputation of Australian organisations. In 2021–22, ransomware groups stole and released the personal information of hundreds of thousands of Australians as part of their extortion tactics. The cost of ransomware extends beyond the ransom demands, and may include system reconstruction, lost productivity, and lost customers.
- **Worldwide, critical infrastructure networks are increasingly targeted.** Both state actors and cybercriminals view critical infrastructure as an attractive target. The continued targeting of Australia's critical infrastructure is of concern as successful attacks could put access to essential services at risk. Potential disruptions to Australian essential services in 2021–22 were averted by effective cyber defences, including network segregation and effective, collaborative incident response.
- **The rapid exploitation of critical public vulnerabilities became the norm.** Australian organisations, and even individuals, were indiscriminately targeted by malicious cyber actors. Malicious actors persistently scanned for any network with unpatched systems, sometimes seeking to use these as entry points for higher value targets. The majority of significant incidents ACSC responded to in 2021–22 were due to inadequate patching.

In the face of rising threats to the digital-dependent Australian economy, cyber defence must be a priority for all Australians. The most effective means of defending against cyber threats continues to be the implementation of the Essential Eight cyber security strategies. To support this, the ACSC launched several new initiatives in 2021–22 to improve Australia's cyber resilience, such as a Cyber Threat Intelligence Sharing (CTIS) platform which automates sharing of indicators of compromise. The Australian Government's ten year investment in ASD, known as REDSPICE, will further harden Australia's cyber defences in 2022–23 and beyond.

What the ACSC saw:

An increase in financial losses due to BEC to over **$98 million**

an average loss of **$64,000** per report.

A rise in the average cost per cybercrime report to over **$39,000** for small business, **$88,000** for medium business, and over **$62,000** for large business

an average increase of **14 per cent**.

A **25 per cent increase** in the number of publicly reported software vulnerabilities

(Common Vulnerabilities and Exposures – CVEs) worldwide.

Over **76,000** cybercrime reports

an increase of **13 per cent** from the previous financial year.

What the ACSC saw:

A cybercrime report every **7** minutes on average

compared to every **8** minutes last financial year.

Over **25,000** calls to the Cyber Security Hotline

an average of **69 per day** and an increase of **15 per cent** from the previous financial year.

150,000 to 200,000 Small Office/Home Office routers in Australian homes and small businesses vulnerable to compromise

including by state actors.

Fraud, online shopping and online banking

were the top reported cybercrime types, accounting for **54 per cent** of all reports.

What the ACSC did:

Responded to over **1,100** cyber security incidents.

Blocked over **24 million** malicious domain requests

through the Australian Protective Domain Name System.

Took down over **29,000** brute force attacks against Australian servers

through the Domain Takedown Service.

Took down over **15,000** domains hosting malicious software

targeting Australia's COVID-19 vaccine rollout.

Shared over **28,000** indicators of compromise with ACSC Partners

through the Cyber Threat Intelligence Sharing platform.

What the ACSC did:

Collaborated with partners on **5** successful operations against criminal online marketplaces and foreign scam networks.

Responded to **135** ransomware incidents

an increase of over **75 per cent** compared to 2019–20.

Notified **148** entities of ransomware activity on their networks.

Conducted **49** high priority operational tasks in response to identified and potential significant cyber threats

including scanning for vulnerable Australian devices.

Published **49** Alerts and **14** Advisories on cyber.gov.au

which collectively saw more than **393,000** visits.

What the ACSC did:

Issued an Advisory urging Australian organisations to adopt an enhanced security posture following Russia's invasion of Ukraine

which was updated **10** times and received more than **57,000** views, plus a potential reach of almost 1 million people through social media.

Briefed more than **200** government, business and critical infrastructure organisations

on the risk of collateral damage to Australian networks following the Russian invasion of Ukraine.

Published **13** new Step-by-Step Guides

to help Australian individuals and small businesses to implement simple cyber security practices.

Expanded the Partnership Program

to over **2,300** network partners, **3,400** business partners, and over **82,000** home partners.

What the ACSC did:

Led **24** cyber security exercises

involving over **280 organisations** to strengthen Australia's cyber resilience.

Operationalised amendments to the *Security of Critical Infrastructure Act*

including through new incident categorisation thresholds and changes to the ReportCyber website.

Notified **5** critical infrastructure entities of malicious cyber activity and vulnerabilities

potentially impacting their networks since the implementation of amendments to the *Security of Critical Infrastructure Act.*

Completed the Critical Infrastructure Uplift Program (CI-UP) pilot

and rolled out activities and tools open to all critical infrastructure partners.

What should individuals do?

Follow the ACSC's easy steps to secure your devices and accounts including:

Update your devices

and replace old devices that do not receive updates

Activate multi-factor authentication

Regularly backup your devices

Set secure passphrases

Watch out for scams

Sign-up to the ACSC's free Alert Service

Report cybercrime to the ACSC

at cyber.gov.au

What should organisations do?

For larger organisations:

implement the ACSC's Essential Eight mitigation strategies, Strategies to Mitigate Cyber Security Incidents and the Information Security Manual.

For smaller organisations:

follow the ACSC's advice for ransomware, Business Email Compromise and other threats.

Review the cyber security posture of remote workers

and their use of communication, collaboration and business productivity software.

Patch vulnerabilities within 48 hours.

If you cannot achieve this, consider using a cloud service provider or managed service provider (MSP) that can.

Only use reputable cloud service providers and managed service providers

that implement appropriate cyber security measures.

Sign-up to become an ACSC partner

to receive insights, advisories and advice.

Test your cyber security detection, incident response, business continuity and disaster recovery plans.

Report all cybercrime and cyber security incidents to the ACSC

via ReportCyber.

Chapter 1

Cybercrime and cyber security incident statistics

- Cyber security incidents responded to by the ACSC are growing in severity.
- Cybercrime has a significant impact on organisations of all sizes; in 2021–22 the average loss per report across businesses increased 14 per cent compared to 2020–21.
- Cybercrime and cyber security incidents remain underreported and the ACSC urges Australian organisations and individuals to report all cybercrimes and cyber security incidents.

Cybercrime and cyber security incident statistics

A cybercrime is an offence committed through or against information and communications technology (ICT). Cybercrimes are either cyber enabled (using ICT to facilitate offences such as fraud or sexual exploitation) or cyber dependent (crimes which can only be committed via ICT, such as the use of ransomware or other malware).

A cyber security incident is an event, or series of events, that has a significant probability of compromising an organisation's operations. Not all cybercrimes lead to cyber security incidents, and the following statistics are from 2 distinct datasets: cybercrimes reported to ReportCyber, and cyber security incidents to which the ACSC responded.

The cost of cybercrime

As the volume of cybercrime increases, cybercriminal methodology evolves, and digital transactions blur national borders, it is becoming increasingly difficult to accurately estimate the total cost of cybercrime.

Cybercrime can cause financial and reputational damage, disrupt business and essential services, and result in permanent damage to an organisation. Self-reported financial loss data as submitted to ReportCyber only captures a small portion of the total financial impact of cybercrime. It does not capture the cost to the customers of victims, nor the capital and recurring costs of cyber security incident remediation.

Frequency of cybercrime reports

During the 2021–22 financial year, over 76,000 cybercrime reports were made via ReportCyber, an increase of nearly 13 per cent from the previous financial year. One cybercrime report is made approximately every 7 minutes, compared to one report every 8 minutes in 2020–21.

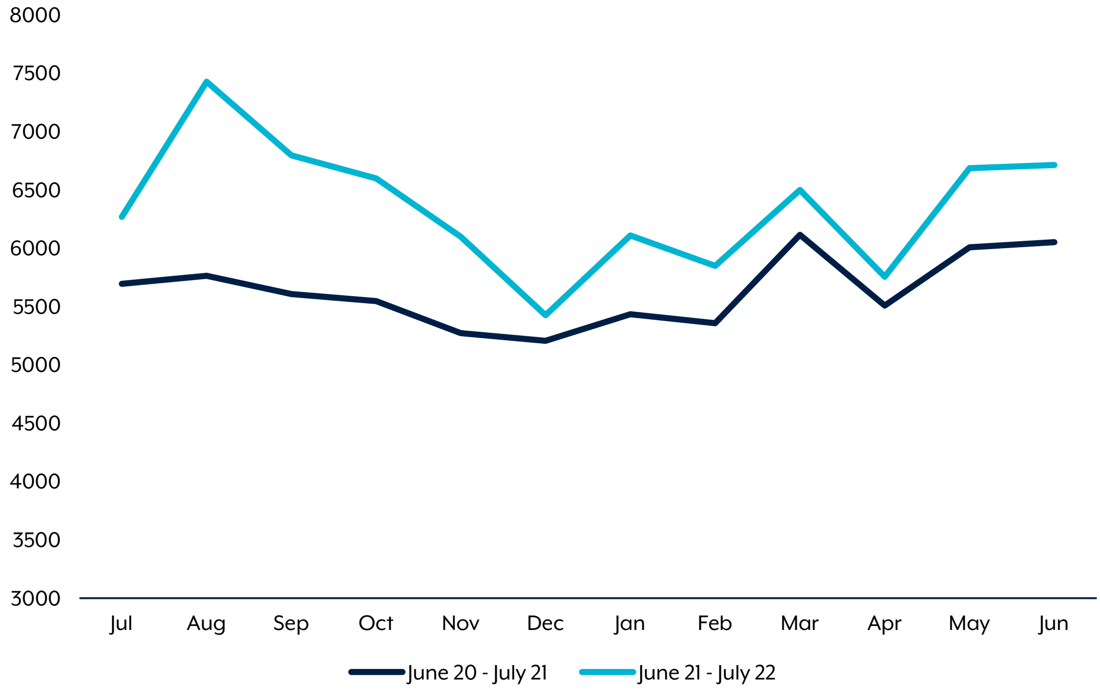


Figure 1: Cybercrime reports by month for 2021–22 financial year compared with 2020–21 financial year

Cybercrime reports by state and territory

Australia's more populous states continue to report more cybercrime. Queensland and Victoria report disproportionately higher rates of cybercrime relative to their populations. However, the highest average reported losses were by victims in the Northern Territory (over $40,000 per cybercrime report where a financial loss occurred) and Western Australia (over $29,000).

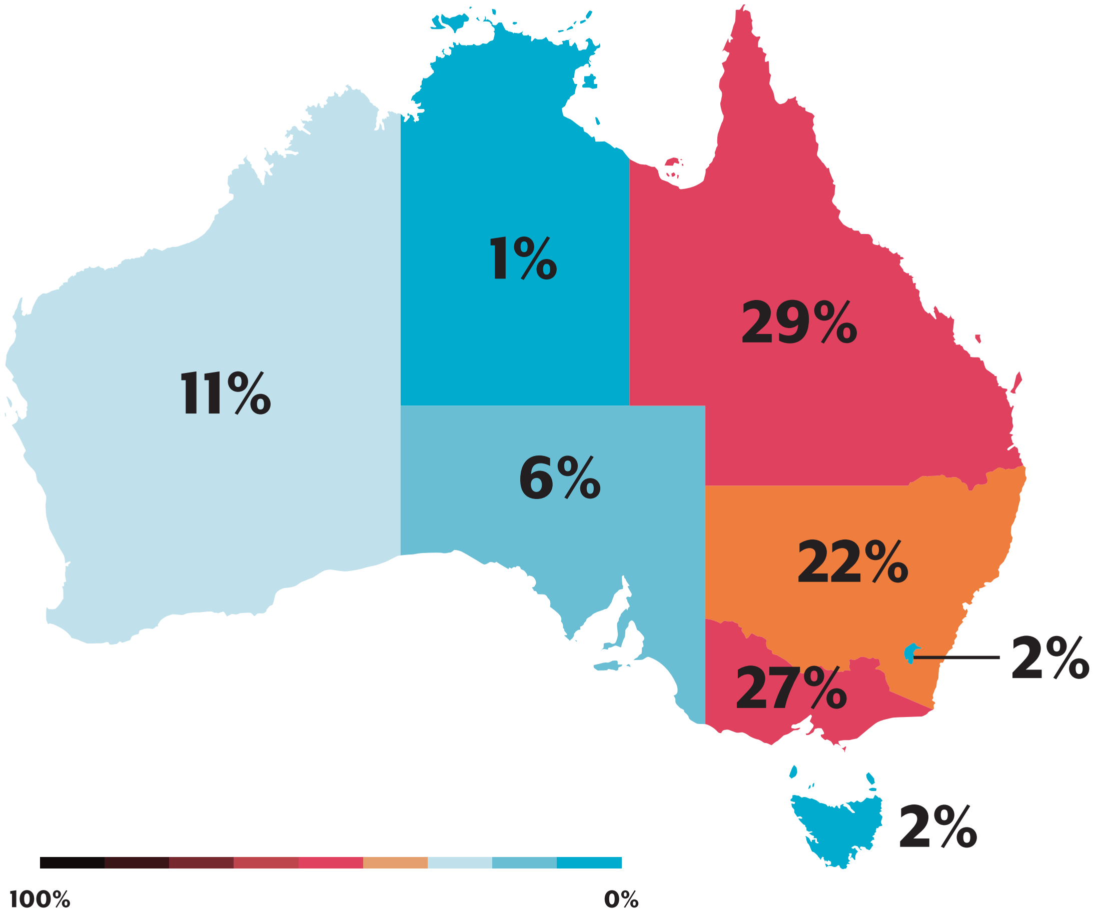


Figure 2: Breakdown of cybercrime reports by assigned jurisdiction for financial year 2021–22

Note: Assigned jurisdiction is the state or territory law enforcement agency assigned to each ReportCyber report. This may differ from the physical location of the victim.

Cybercrime by type

The most frequently reported cybercrimes were all cyber enabled crimes:

- online fraud: approximately 27 per cent
- online shopping: approximately 14 per cent
- online banking: approximately 13 per cent.

Cyber dependent crimes, such as ransomware, were a very small percentage of total cybercrime reports. Nevertheless, the ACSC assesses that ransomware remains the most destructive cybercrime threat. This is because ransomware has a dual impact on victim organisations—their business is disrupted by the encryption of data, but they also face reputational damage if stolen data is released or sold on. The public are also impacted by disruptions and data breaches resulting from ransomware.

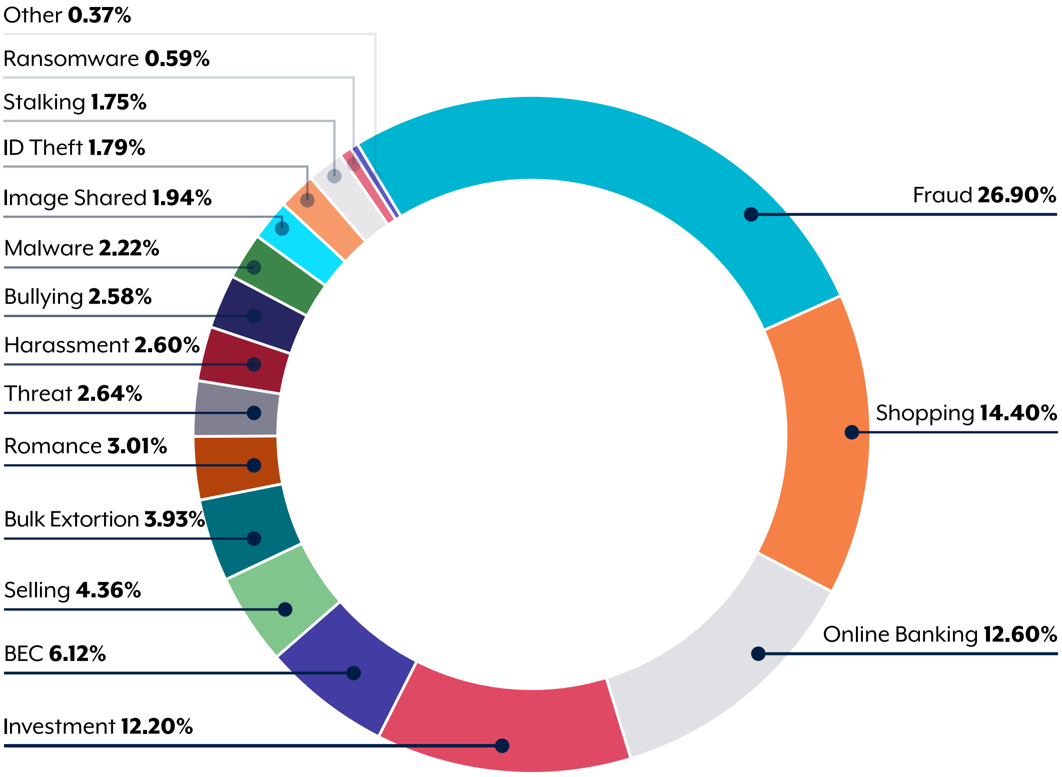


Figure 3: Cybercrime reports by type for financial year 2021–22

Cybercrime loss by organisation size

Medium-sized businesses (defined by Australian Bureau of Statistics as between 20 and 199 employees) had the highest average loss per cybercrime report where a financial loss occurred.

This may be because they were less likely than large organisations to apply cyber security mitigations as outlined in the ACSC's Strategies to Mitigate Cyber Security Incidents. These strategies decrease the likelihood and impact of cyber incidents. In addition, medium-sized organisations may be more likely to report cybercrime to ReportCyber, as they are less likely than larger organisations to have sufficient in-house or commercial incident response capabilities. The ACSC urges organisations to report all cybercrime, irrespective of the financial loss incurred, as it helps to better understand and defend against the threat.

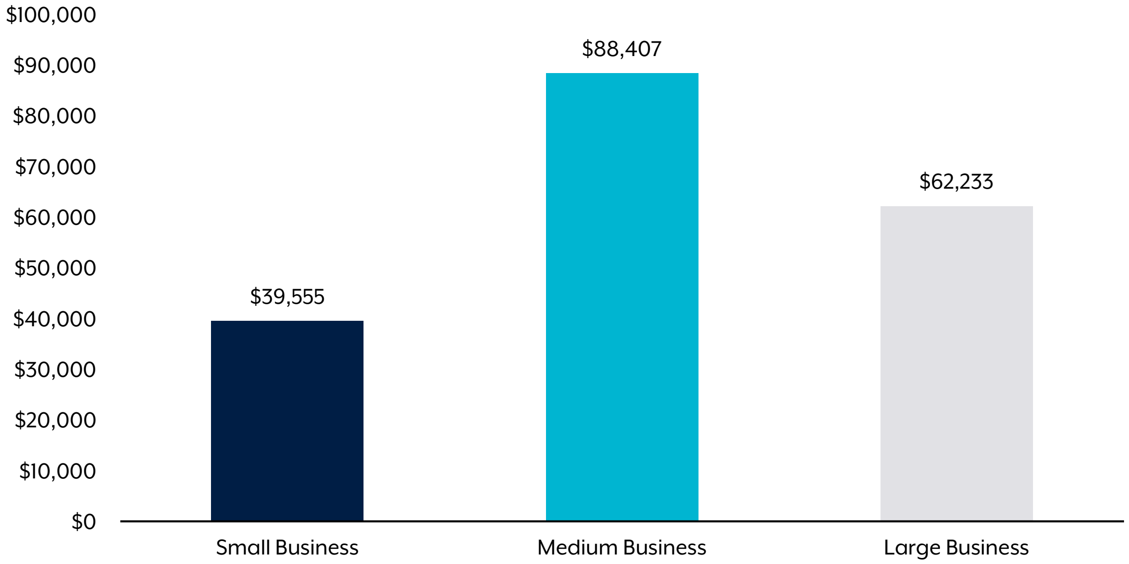


Figure 4: Cybercrime reports and average reported loss by organisation size for financial year 2021–22

Note: The 2021 Annual Cyber Threat Report averaged financial loss across all cybercrime reports. This year's Report averages only those cybercrime reports where financial loss occurred. The ACSC assesses that excluding reports where no financial loss occurred provides more accurate and actionable data for businesses.

Calls to the ACSC

The number of calls to 1300 CYBER1 has continued to increase. The ACSC received more than 25,000 calls in the 2021–22 financial year, an average of 69 calls per day. This is a 15 per cent increase on the 2020–21 financial year and over a four-fold increase from the 2019–20 financial year, when the ACSC received 5,300 calls.

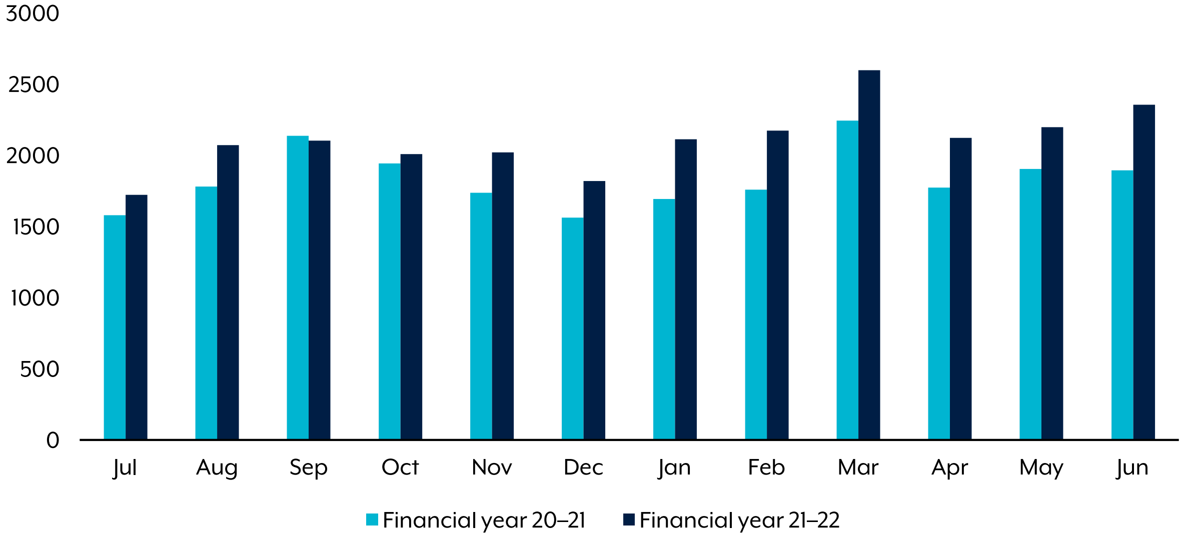


Figure 5: Call volumes for financial year 2021–22 compared with financial year 2020–21

Cyber security incidents

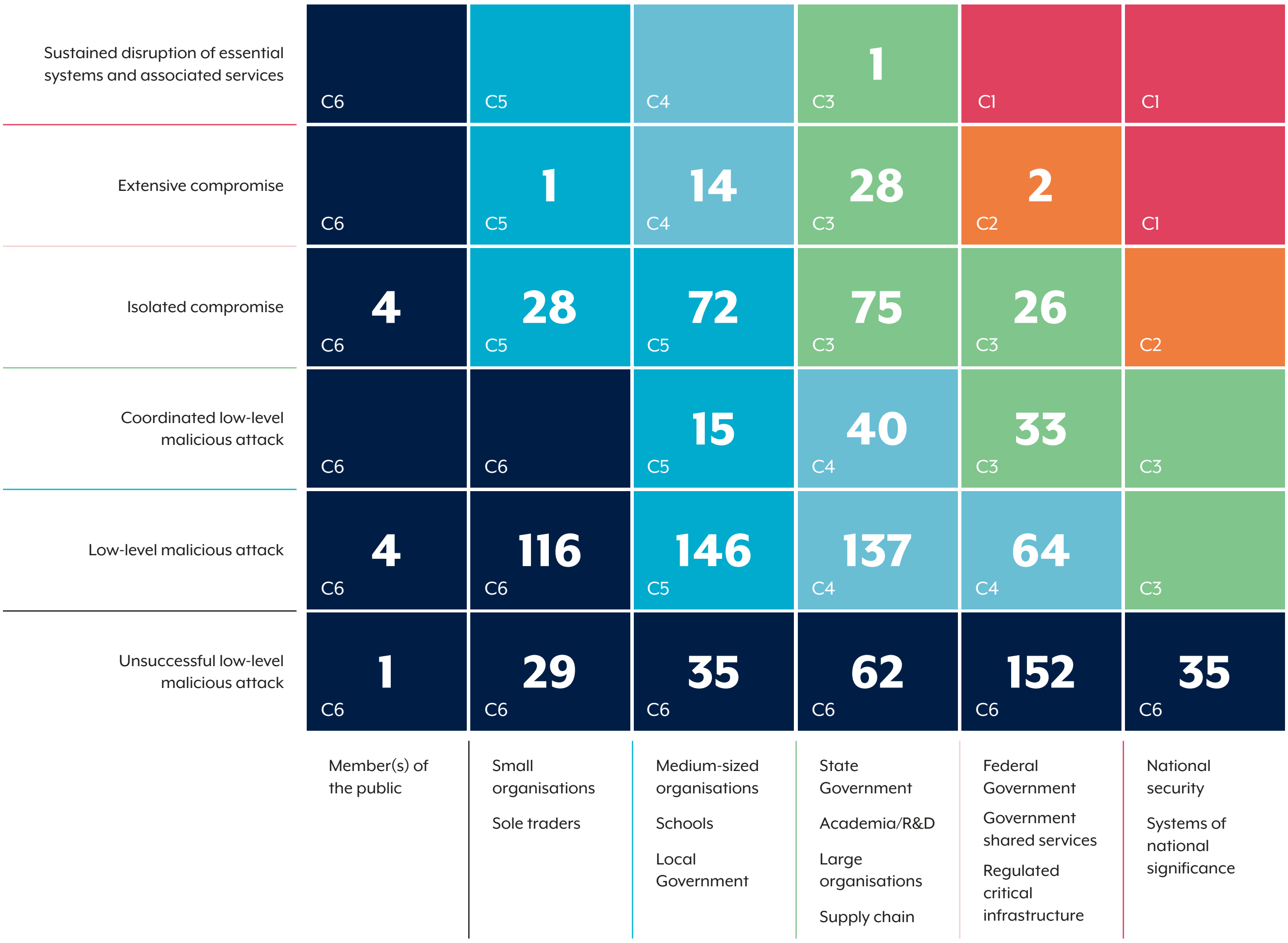
During the 2021–22 financial year, the ACSC responded to over 1,100 cyber security incidents, an average of 21 cyber security incidents per week. Compared to the 2020–21 financial year, this is a decrease of 36 per cent. This does not mean that the cyber security threat to Australian organisations has decreased, especially as the number of cybercrime reports has increased. The expansion of Australia's commercial incident response sector means incidents which may have previously required an ACSC response may now be being handled by in-house or contracted incident response teams.

Cyber security incident severity

The ACSC categorises each incident it responds to on a scale of Category 1, the most severe, to Category 6, the least severe. Incidents are categorised on severity of effect, extent of compromise, and significance of the organisation.

The number and severity of cyber security incidents in the 2021–22 financial year is not directly comparable with previous financial years, as the ACSC introduced a new incident categorisation scale in March 2022. This was due to the introduction of mandatory incident reporting for Regulated Critical Infrastructure under amendments to the *Security of Critical Infrastructure Act 2018* (SoCI Act). Changes included simplifying the scale, prioritising incidents related to Critical Infrastructure and Systems of National Significance networks and refining definitions of cyber effects and impacts.

The severity of cyber security incidents is increasing. Nearly 15 per cent of incidents in the 2021–22 financial year were categorised as C3, up from approximately 6 per cent in the previous financial year. This is partly attributable to the category changes, but also to an increase in attacks by cybercriminals on larger organisations and an increased impact on victims. Attacks included the exfiltration of sensitive data and the movement by malicious actors across multiple segments of affected networks.



	Member(s) of the public	Small organisations Sole traders	Medium-sized organisations Schools Local Government	State Government Academia/R&D Large organisations Supply chain	Federal Government Government shared services Regulated critical infrastructure	National security Systems of national significance
Sustained disruption of essential systems and associated services	C6	C5	C4	1 C3	C1	C1
Extensive compromise	C6	1 C5	14 C4	28 C3	2 C2	C1
Isolated compromise	4 C6	28 C5	72 C5	75 C3	26 C3	C2
Coordinated low-level malicious attack	C6	C6	15 C5	40 C4	33 C3	C3
Low-level malicious attack	4 C6	116 C6	146 C5	137 C4	64 C4	C3
Unsuccessful low-level malicious attack	1 C6	29 C6	35 C6	62 C6	152 C6	35 C6

Figure 6: Cyber security incidents by incident category for financial year 2021–22

Cyber security incidents by sector

Excluding government sectors—which have some additional reporting obligations—the health care and social assistance sectors reported the highest number of cyber security incidents during the 2021–22 financial year. Compared to the 2020–21 financial year, the retail sector dropped out of the top 10, replaced by the electricity, gas, water and waste service sector.

The top 10 reporting sectors accounted for approximately 75 per cent of all incidents for the 2021–22 financial year. As such, these sectors are a focus for ACSC partnership and outreach activities.

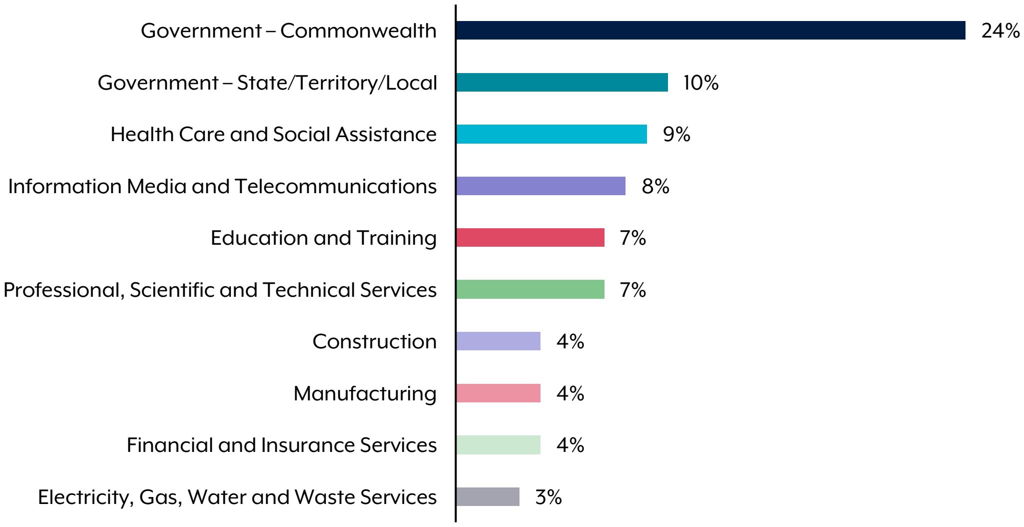


Figure 7: Cyber security incidents to which the ACSC responded in financial year 2021–22, top 10 industry sectors

Note: The reporting frequency of government agencies is in part due to their obligations to report significant cyber security incidents to the ACSC, and may not necessarily reflect a greater susceptibility to cyber security incidents.

Chapter 2

State actors

- Russia's invasion of Ukraine has increased the cyber threat globally.
- Malicious state actors continue to seek sensitive information, including by targeting Australian small businesses and individuals.
- Most compromises identified by the ACSC used relatively simple tradecraft which could have been prevented by enhanced cyber security.

Gaining a foothold to steal our secrets

In 2021–22, state actors continued to engage in malicious cyber operations as an efficient method of political and economic espionage. State actors seek sensitive information—including personally identifiable information (PII)—to support their government's intelligence requirements. But these actors do not just want classified information. They also want to understand who we are, how we connect with each other, and what values we hold. Furthermore, in some cases, they may seek to pre-position in strategic networks to prepare for coercive or disruptive activity against us.

Over the past financial year, Australia continued to be the target of persistent cyber espionage by a wide range of state actors due to its regional and global interests, international partnerships and participation in multilateral forums. This cyber espionage is often conducted or directed by foreign intelligence services seeking information from public and private networks across Australia, including political, diplomatic, military, technological and commercial data, as well as personal data from individual Australians.

The ACSC collaborated with Australian, state and territory government agencies to ensure events such as the Census and state and federal elections were resilient to malicious cyber activity by state or criminal actors.

Case Study: ACSC support to the Census

The Australian Bureau of Statistics (ABS) ran the Census in August 2021. ABS systems are an attractive target for malicious actors, including state actors, as they hold personal information about Australians.

The ABS was particularly concerned with maintaining the availability of the Census systems, the confidentiality of Australians' information, and the integrity and utility of the collected data. The ACSC provided a range of services to the ABS to assess and improve the cyber security of its systems.

Prior to the Census, the ACSC provided ABS with threat intelligence briefings. The ACSC also employed its active cyber defence capabilities to assess and pre-empt malicious cyber activity against the Census.

The ACSC conducted a review of ABS systems, including a source code review and penetration testing to detect cyber security vulnerabilities, and analysis to detect if there was malicious activity already on the system. Recommendations resulting from the review were provided to the ABS.

Throughout the Census, the ACSC monitored ABS systems to help detect and respond to threats. On Census night, the ACSC provided on-site operational support to bolster any critical incident response.

The ACSC found no indication of malicious activity through its assessments, and critical cyber security recommendations were resolved by the ABS prior to the Census. The Census was completed without any cyber security incident or disruption to services.

While state actors have access to a wide range of sophisticated and bespoke capabilities, the majority of compromises the ACSC observed used relatively simple tools and techniques. These include spear phishing, targeting third-party service providers and exploiting unpatched or misconfigured systems using public vulnerabilities. The exploitation of public vulnerabilities is low cost and scalable, and exploits can be deployed within hours of a patch release or technical write up. Exploiting public vulnerabilities also avoids the need to use zero-day exploits—vulnerabilities that have not been disclosed or patched by the software vendor—allowing state actors to preserve these for use against the highest value targets. State actors will likely continue to use simple tools and techniques to target government and business networks for as long as it remains effective, inexpensive and scalable.

Cyber operations as a geostrategic tool

The Indo-Pacific is at the centre of geostrategic competition, and cyber operations are a valuable tool in this contest. Some countries use cyber operations to gain advantage by stealing other nations' security secrets and intellectual property at a greater scale than in the past. They can also use cyberspace to sow disinformation, interfere in economies and shape public sentiment. If necessary, states can launch cyberattacks that sabotage and destabilise their adversaries. Much of this can be done covertly, at relatively low cost and in ways that make it hard for other states to deter or respond.

Cyberspace itself has become a battleground. Some countries in our region continue to strain the norms and institutions that govern cyberspace as a global commons. These countries have increasingly cut access to the open internet and used digital tools to repress freedoms. These countries seek to export their approach and impose it on others by undermining international standards and technical protocols. Australia opposes these actions and is committed to a free and open Internet. In April 2022, Australia joined over 60 other nations in launching A Declaration for the Future of the Internet, which describes our position on the potential for digital technologies to uphold the values that promote connectivity, democracy, and the rule of law.

Cyberspace is also a joint warfighting domain, with cyber effects increasingly incorporated into military operations. Some countries are acquiring cyber capabilities which can 'hold-at-risk' the networks other countries rely on. To 'hold-at-risk' is to demonstrate the capability to overcome the defences of another country, to undermine confidence in networks and enable state actors to cripple essential services in the event of a conflict.

Cyber operations in military conflict

Russia's invasion of Ukraine has altered the geopolitical balance in ways that could expose organisations to increased malicious cyber activity.

Ukrainian government officials have acknowledged they are fighting a dual war—one on the ground and one in the digital realm. Cyber operations have been used as a tool of war alongside a major ground offensive, with malicious cyber activity against Ukrainian networks before and during the conflict.

Ukraine has experienced an onslaught of sustained disruptive cyber activity, including distributed denial of service (DDoS) attacks. While the impact of this malicious activity has been mitigated by Ukraine's cyber defensive measures, it still has the potential to cripple essential services and have cascading effects. In the first 6 weeks of the invasion, at least 8 variants of destructive malware were identified, including wiper malware designed to erase data and prevent computers from booting.

Against this backdrop, the integration of cyber operations into conventional war has drawn non-traditional combatants and civilian entities into the conflict. Criminal syndicates and issue-motivated groups have conducted activities in support of Russian or Ukrainian interests, independent of Russian and Ukrainian government chains of command. Issue-motivated groups have made claims of successful attacks against government and private networks, including exfiltration and posting of data on the darkweb. Such activities facilitate future potential cyberattacks by malicious state and non-state actors.

Pages 30 and 31 record a subset of the malicious cyber activity which occurred in the first 60 days of the war. Disruptive activities continue unabated, and escalating geopolitical tensions will likely see the continued use of cyber effects as a means of dissuasion, disruption, degradation or denial.

Cyber risks to Australian networks

Russia's invasion of Ukraine demonstrated the real threat of disruptive and destructive cyber operations, including the potential for third parties to suffer collateral damage. Some Russian cyber operations impacted beyond their primary target sets. For example, a 24 February 2022 attack on a satellite communications company had spillover effects across geographic borders. In addition to causing outages across Ukraine, this attack disabled over 10,000 satellite communications terminals outside Ukraine, including terminals that supported the operation of wind turbines and internet services for private citizens.

Previous cyberattacks against Ukraine have also had international consequences—such as the NotPetya malware in 2017, which affected companies worldwide, including in Australia. Russian cyber actors may conduct malicious activity as a response to military materiel support provided by the US, UK, Australia and other partners, as well as the economic costs imposed on Russia.

Australia would be vulnerable in future regional or global conflicts to cyber operations that target the supply chains that Australian systems depend upon. This would be the case even if Australia were not directly involved. There would probably be little warning of such disruption. Australian network owners need to consider how to secure their critical systems and protect their sensitive information; for instance, through improved segmentation between their corporate and operational networks.

What the ACSC is doing

In the lead-up to the invasion, DDoS attacks targeted Ukraine's finance sector and banks. On 20 February 2022, Australia joined the US and UK in publicly attributing these cyberattacks to the Russian General Staff Main Intelligence Directorate.

On 23 February 2022, the ACSC released an Alert and an Advisory urging Australian organisations to urgently adopt enhanced cyber security postures by prioritising the following actions:

- patching applications and devices
- implementing mitigations against phishing and spear phishing attacks
- ensuring that logging and detection systems are fully updated and functioning
- reviewing incident response and business continuity plans.

In cooperation with our international partners from Canada, New Zealand, the UK and the US, on 21 April 2022, the ACSC released a joint Advisory specifically on Russian state and cybercriminal threats to critical infrastructure. The Advisory urges critical infrastructure network operators to prepare for and mitigate potential cyber threats by hardening their cyber defences and performing due diligence to identify indicators of compromise.

In addition, the ACSC has increased engagement with international partners to share tactics and techniques, and worked closely with industry partners to share knowledge of the threat environment. The ACSC briefed more than 200 business organisations on the risk of collateral damage to Australian networks following the Russian invasion of Ukraine, and has also provided multi-classification threat briefings to government and critical infrastructure partners.

Beyond the immediate threat presented by Russia's invasion of Ukraine, the ACSC works to counter the risk of malicious activity by a wide range of state actors.

By the end of the 2021–22 financial year, the Advisory had been updated **10** times.

received more than **57,000** views,

and had a potential reach of more than **950,000** users through ACSC's social media platforms.

Malicious cyber activity in first 60 days of Russia's invasion of Ukraine

Europe

Whole of economy

- DDoS attack against major Telecommunications provider
- Phishing campaigns launched against European citizens

Government

- Phishing campaign against European governments and militaries
- Phishing campaign targeting officials helping evacuate Ukrainian refugees

Ukraine

Whole of economy

- Ransomware attacks on Ukrainian citizens
- DDoS causes severe outages to Media and Telecommunications sector
- Phishing campaign targeting Ukrainian media

Government

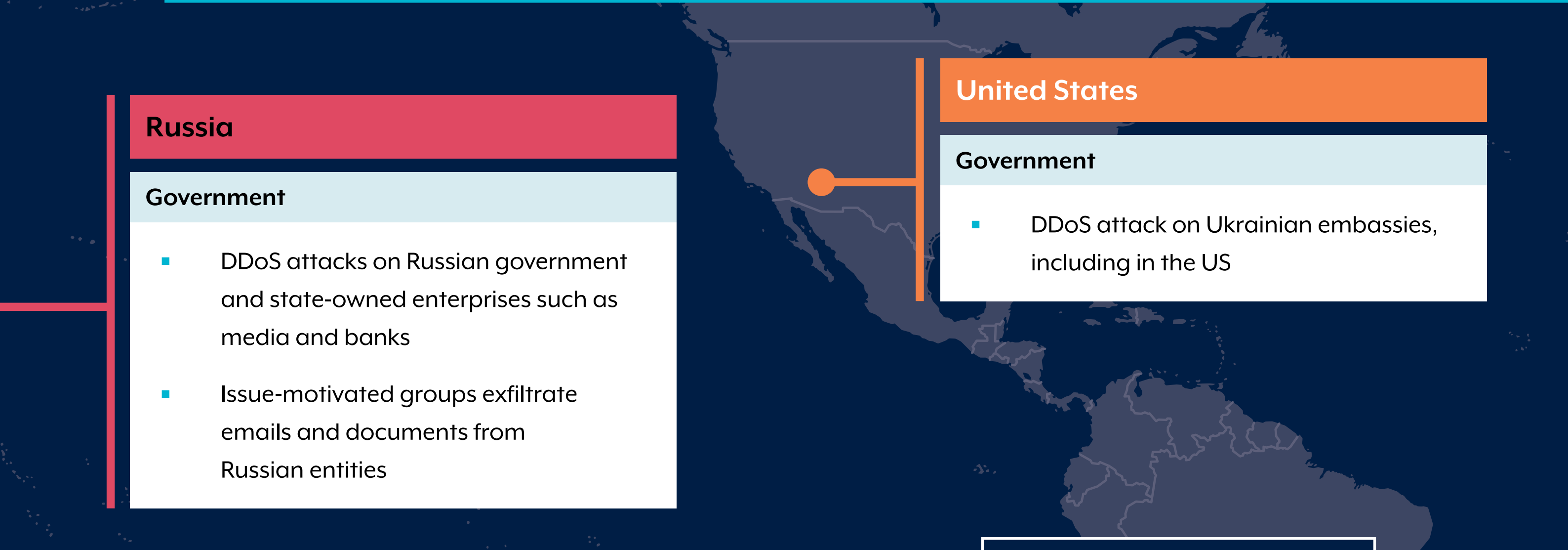
- Malware and DDoS attacks on Ukrainian government departments
- Mass phishing campaign against Ukrainian government and military personnel

Russian state-sponsored cyber actors

Russian state-sponsored cyber actors have demonstrated capabilities to compromise ICT networks, develop mechanisms to maintain long-term, persistent access to ICT networks, exfiltrate sensitive data from ICT and Operational Technology (OT) networks, and disrupt critical infrastructure systems and OT functions by developing destructive malware.

Numerous Russian government and military organisations have the capability to undertake cyber operations against ICT and OT networks, including elements of:

- The Russian Federal Security Service (FSB)
- The Russian Foreign Intelligence Service (SVR)
- The Russian General Staff Main Intelligence Directorate (GRU)
- The Russian Ministry of Defence



Russia

Government

- DDoS attacks on Russian government and state-owned enterprises such as media and banks
- Issue-motivated groups exfiltrate emails and documents from Russian entities

United States

Government

- DDoS attack on Ukrainian embassies, including in the US

What you should do

How to protect yourself from state actors

Individuals and organisations are not just targeted for their own data holdings; their networks can be weaponised against others. For example, in 2021–22 personal devices and small office or home office (SOHO) routers were used by foreign intelligence services to conduct espionage and theft of intellectual property. Malicious actors can use these routers to conduct person-in-the-middle compromises or as a vector to target other networks. The ACSC estimates that at least 150,000 to 200,000 devices in Australian homes and small businesses are vulnerable.

Small businesses and individuals should prioritise automated updates, which help prevent network compromises by even the most sophisticated actors. The ACSC also provides step-by-step guides to secure your accounts and devices at cyber.gov.au. Larger organisations should continue to implement the Essential Eight cyber security strategies.

REDSPICE

- The global strategic environment is deteriorating.
- The rapidly advancing technological landscape presents great opportunities but also serious threats.
- Cyberspace is of increasing importance to warfare and national security.

REDSPICE (Resilience, Effects, Defence, SPace, Intelligence, Cyber, Enablers) will be pivotal to addressing future cyber threats. REDSPICE will expand the range and sophistication of ASD's intelligence, offensive and defensive cyber capabilities, and deliver forward-looking capabilities essential to maintaining Australia's strategic advantage and capability edge over the coming decade and beyond. It will:

- help anticipate and prevent a crisis
- block sophisticated cyberattacks against Australian critical infrastructure
- provide offensive capabilities that equip government with retaliatory options
- ensure Australia's cyber and intelligence capabilities remain resilient to attack.

3X current offensive cyber capability

2X persistent cyber-hunt activities

The REDSPICE investment will help train a new generation of cyber and intelligence experts to protect Australia from cyber adversaries.

1900 new analyst, technologist, corporate, and enabling roles across Australia and the world

Analysts

Create our edge, solve the problems others cannot.

Technologists

Use emerging and cutting-edge technology and big data to solve complex problems.

Corporate & Enabling Services

Enable our purpose.

A nationally and internationally distributed workforce will create additional redundancy in ASD's critical capabilities and opportunities for greater partnership with industry, academia and other sectors of the Australian economy.

40%

staff located outside Canberra

4X

global

footprint

REDSPICE will provide new intelligence capabilities and build our threat intelligence picture, including through threat intelligence sharing with ACSC partners.

Enhanced National Cyber Defence

- Improves resilience of critical infrastructure against sophisticated cyber attacks
- Increases the visibility of threats to Australia's most critical systems
- Improves machine-time cyber threat intelligence sharing across government and industry
- Doubles persistent cyber-hunt activities and nationwide cyber-incident response.

REDSPICE provides $5 billion in opportunities for Australian industry, including small and medium Australian enterprises. This will grow the wider Australian cyber security sector.

Chapter 3

Cybercrime

- Cybercrime continues to pose a high threat to Australia’s economic and social prosperity.
- Cybercriminals are increasingly persistent in targeting all sectors of Australia’s economy.
- Compromises trended towards targeting high value transactions like property settlements.

Proliferation of threats

Australia is an attractive target for cybercriminals. Our widespread internet connectivity, per-capita wealth, and investment structures—such as moveable superannuation accounts and widespread share ownership—are all powerful incentives for cybercriminals.

During the 2021–22 financial year, fraud, financial and identity theft and BEC continued to be common cyber threats due to their volume and ability to cause severe and long-term harm. Many actors used common techniques such as spear phishing to compromise victims' networks.

Australia's cybercrime environment over 2021–22 was underpinned by the constant, rapid evolution of cybercriminal techniques used to target Australia for profit. This evolution was not limited to malware but encompassed all aspects of the cybercriminal environment, including target identification and exploitation, service delivery, cash-out methods, and supporting infrastructure. Ultimately, while cybercrime capabilities became more sophisticated, they also became more accessible for less technologically skilled actors. This ongoing evolution enabled cybercriminals to consistently adapt to environmental changes, while remaining resilient to disruption efforts by law enforcement.

Cybercrime-as-a-Service

The evolution of Cybercrime-as-a-Service (CaaS) continued to increase the overall cybercrime threat to Australia. CaaS encompasses an ever-increasing range of purchasable tools, services and information used to facilitate cybercriminal operations. Examples of CaaS include, but are not limited to, the complicit provision of server infrastructure used to host cybercriminal campaigns, the sale of access to compromised victim networks, money laundering services, and the development and obfuscation of malware. The availability of these enabling functions means that individual actors are not required to be an expert in every component of a criminal operation. In effect, cybercriminals are outsourcing elements of their operations, and a growing black market is serving their needs.

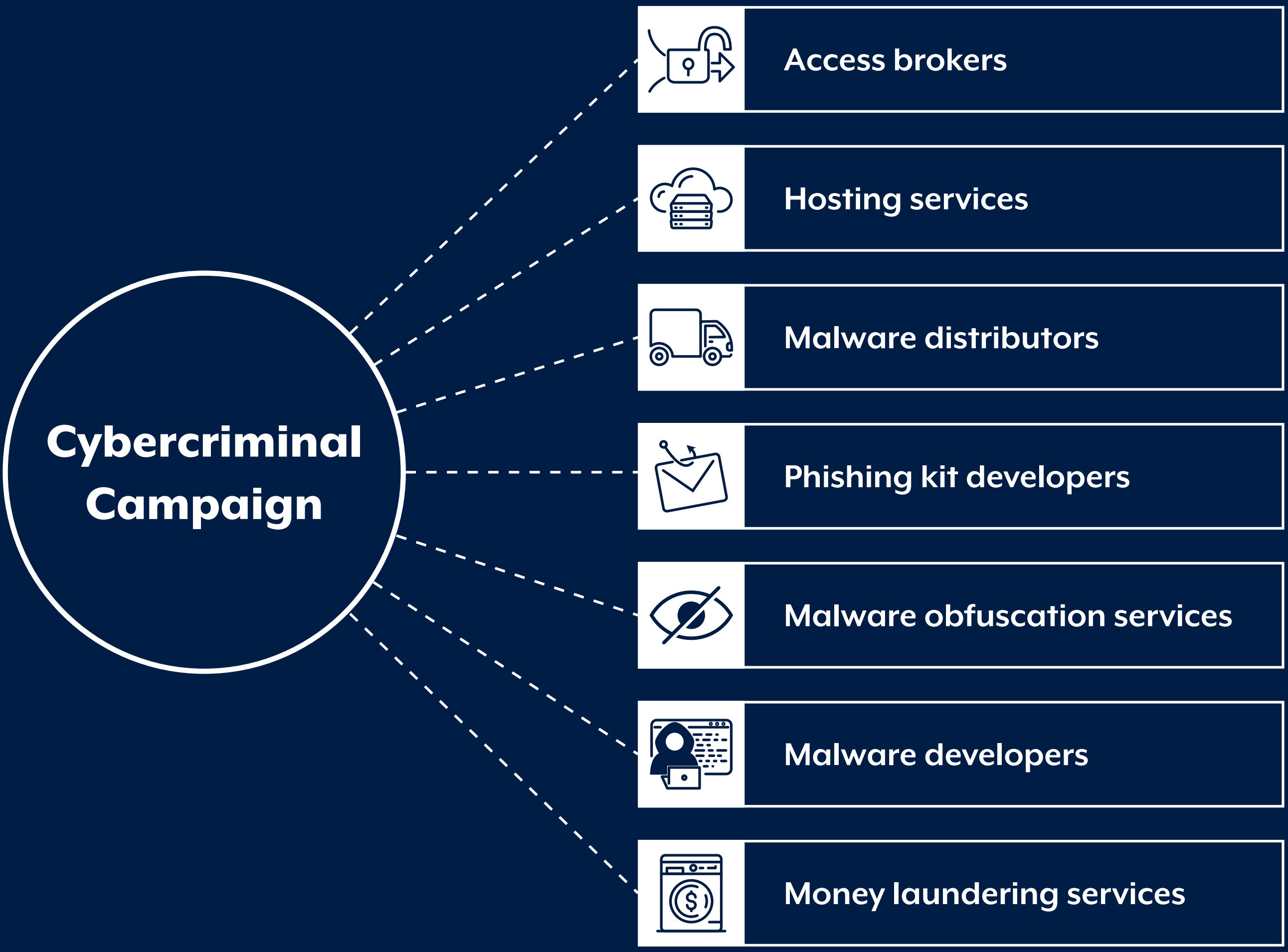


Figure 8: Cybercrime-as-a-Service ecosystem

The expansion of the CaaS industry has lowered the barrier to entry for actors seeking to conduct cybercrime. For instance, Ransomware-as-a-Service (RaaS) provides actors who may not have the technical skill to develop their own ransomware with an opportunity to launch highly profitable attacks. In addition, the CaaS industry allows actors to monetise their expertise in a particular skillset. As a consequence, cybercriminals have become more specialised over 2021–22, and pose a greater threat to Australians and businesses.

During 2021–22, the ACSC collaborated with partners on 5 successful operations against criminal online marketplaces and foreign scam networks. While offshore cybercrime groups have exploited Australian victims, individual actors—including Australian citizens—remain a threat. Australian law enforcement agencies have leveraged international partnerships to tackle criminal behaviour across the globe.

Case Study: Operation Boone

In October 2021, the New South Wales (NSW) Supreme Court ordered the forfeiture of $1.66 million by a 23-year-old Sydney man. This followed his conviction for selling illegally obtained logins for online services such as Netflix. More than $1.2 million of the proceeds were in cryptocurrency, making for the largest seizure of cryptocurrency in Australian history.

This was the culmination of Operation Boone, a five year joint investigation by the AFP and the US Federal Bureau of Investigation (FBI). The Australian man conspired with a US individual to steal the credentials of streaming service customers. The Australian sold the credentials through 4 account-generator websites which had over 150,000 users.

The proceeds were money-laundered through a complex system of PayPal accounts and cryptocurrency wallets. Following an extensive investigation, the AFP seized the cryptocurrency and Paypal accounts and charged the Australian with 5 offences.

Operation Boone demonstrates how the AFP's cybercrime investigation and asset confiscation capabilities work together. The Australian was sentenced to a 2 year, 2 month intensive corrections order, while the confiscated $1.66 million will be reinvested in the Australian community through initiatives that include local crime prevention and drug treatment programs.

For individuals, the case study highlights the importance of not reusing passwords. The theft of streaming service logins relied on credential stuffing—using stolen usernames and passwords to access other services via automated logins. If account owners had used secure passphrases or multi-factor authentication (MFA), their accounts would not have been compromised by the offender.

Business Email Compromise

BEC, where malicious actors compromise organisations via email, continues to be lucrative for cybercriminals. BEC is not limited to scamming businesses out of money or goods. Cybercriminals also use BEC to pretend to be business representatives or to trick employees into revealing confidential business information. BEC is also an entry point for malicious actors to move into higher value targets within networks. The compromise of a single employee email can be a prelude to a major ransomware attack.

In 2021–22, the number of successful BEC reports declined slightly to 1514. However, self-reported losses in 2021–22 increased significantly to over $98 million. Nationally, the average loss per successful BEC increased to over $64,000. The most BEC reports came from Queensland (389 reports), but average self-reported financial losses were highest in Western Australia, at approximately $112,000 per report. Western Australia had several reports of financial losses over $1 million due to BEC, lifting its overall average.

Investigations into BEC suggest property settlements are being targeted. This is likely due to the high value of transactions. Property prices increased further during the coronavirus pandemic and digital settlement methods became more entrenched, making property transactions an attractive target. Despite the best efforts of law enforcement agencies, only a small fraction of BEC financial losses are ever recovered.

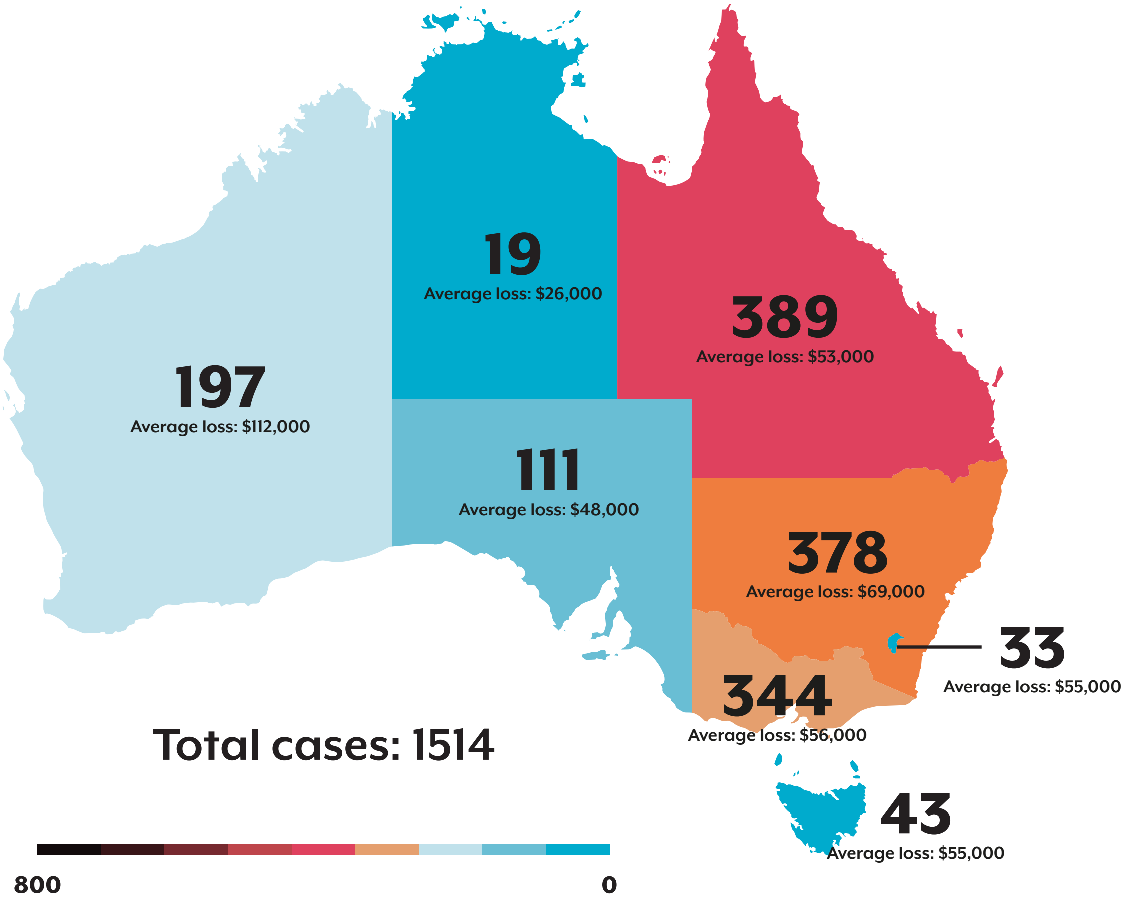


Figure 9: Breakdown of successful BEC reports by jurisdiction for financial year 2021–22

AFP Initiative: Operation Dolos

Operation Dolos is an AFP-led, multi-agency taskforce which counters transnational cybercriminals conducting or facilitating BEC—a cybercrime which commonly crosses borders. Operation Dolos targets and disrupts the BEC crime model, ultimately disrupting transnational organised cybercrime syndicates.

To do this, Operation Dolos works with individual Australians and small to medium businesses that have been targeted by BEC, and disrupts the flow of proceeds to and from BEC syndicates. In December 2021, the AFP announced the arrest of 18 money mules by NSW Police, Victoria Police, and Queensland Police.

In the 2021–22 financial year, Operation Dolos was able to recover over $5.97 million in funds stolen by cybercriminals.

Case study: Falsified invoices via BEC

In July 2021, an Australian financial firm fell victim to BEC, paying over $600,000 on behalf of one of their clients after receiving a falsified invoice. The invoice appeared to be legitimate and from a business that they regularly dealt with, but the bank details had been altered to an account controlled by cybercriminals. The funds were laundered through the purchase of cryptocurrency, gold bullion, cash withdrawals and other purchases.

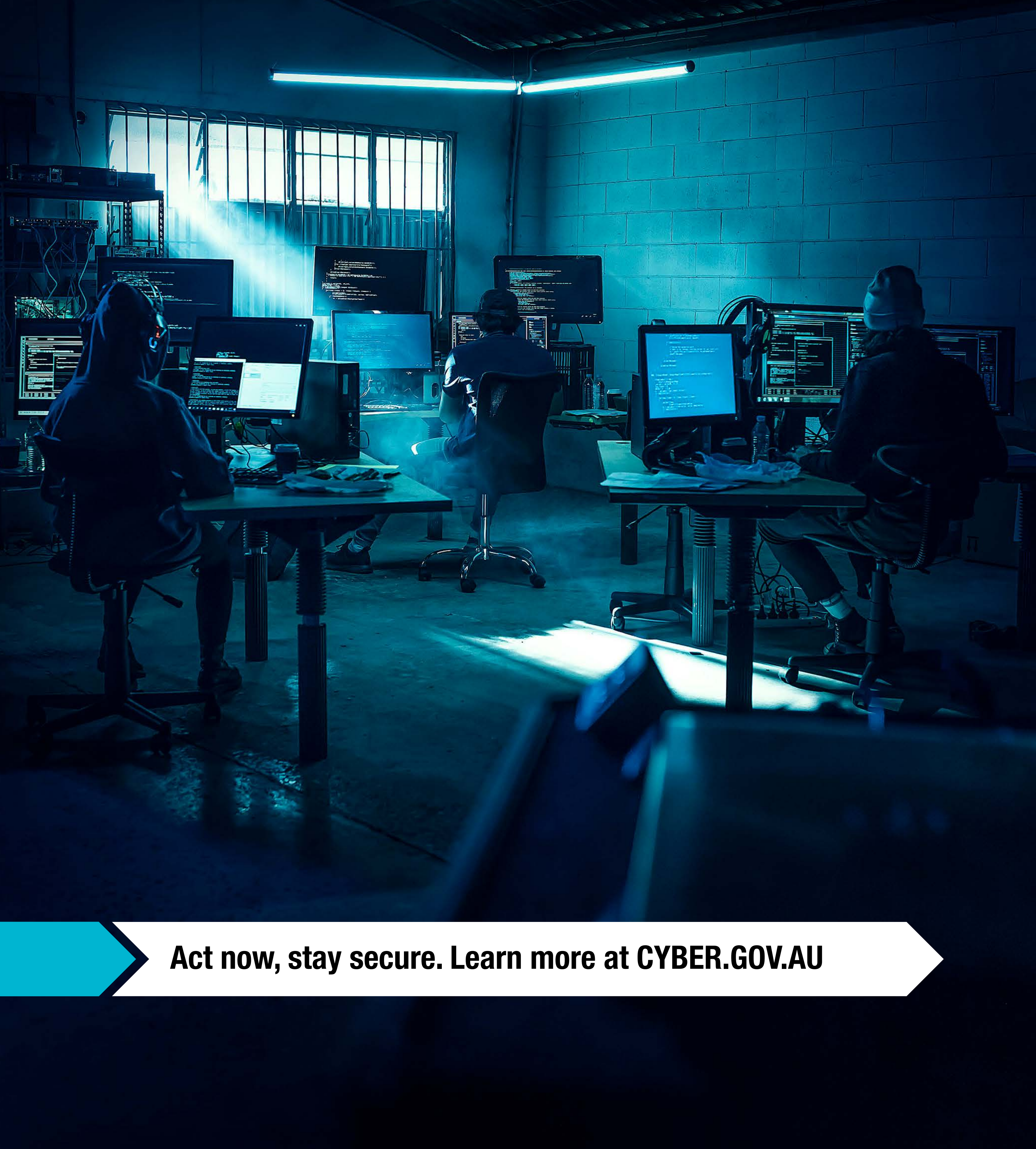
In April 2022, AFP Cyber Command, NSW Police, and Victoria Police conducted a joint activity under Operation Dolos and arrested the member of the syndicate responsible for laundering the proceeds of the crime. Over $140,000 was recovered and returned to the victim.

The case study illustrates the importance of verifying requests for large payments and banking changes, even when they appear to come from businesses with an established reputation. Technical controls such as MFA and secure email gateways can also protect organisations from BEC.

TECHNOLOGY ADVANCES RAPIDLY.

SO DO CYBERCRIMINALS.

Protect yourself against cybercrime.



Act now, stay secure. Learn more at CYBER.GOV.AU

How to protect yourself from cybercrime

Cybercriminals are increasingly persistent in targeting all sectors of Australia's economy. Financial losses divert resources from other areas of critical need. The ACSC seeks to counter this targeting through tailored advice to different sectors of Australian society; for instance through the Act Now, Stay Secure communication and uplift program.

Over the 2021–22 financial year, the Act Now, Stay Secure advertising campaign:

- delivered over 57 million online ads to Australians though social media, video and search
- reached over 6.2 million Australians through broadcast radio advertising
- was supported by an organic social media campaign with a potential reach of 637,000 people
- was amplified by 191 stakeholders sharing campaign content to their own channels.

Act Now, Stay Secure themes

July 2021
Email Security

August 2021
Backups

September 2021
Annual Cyber Threat Report

October 2021
Updates

November 2021
Online Shopping

The launch of the Australian Cyber Security Hotline

The launch of the online learning resources on cyber.gov.au

The launch of the Small Business Cyber Security guide

February 2022
Secure Your Portable Devices

Cyber Security Instruction Manual: A Kid's Guide

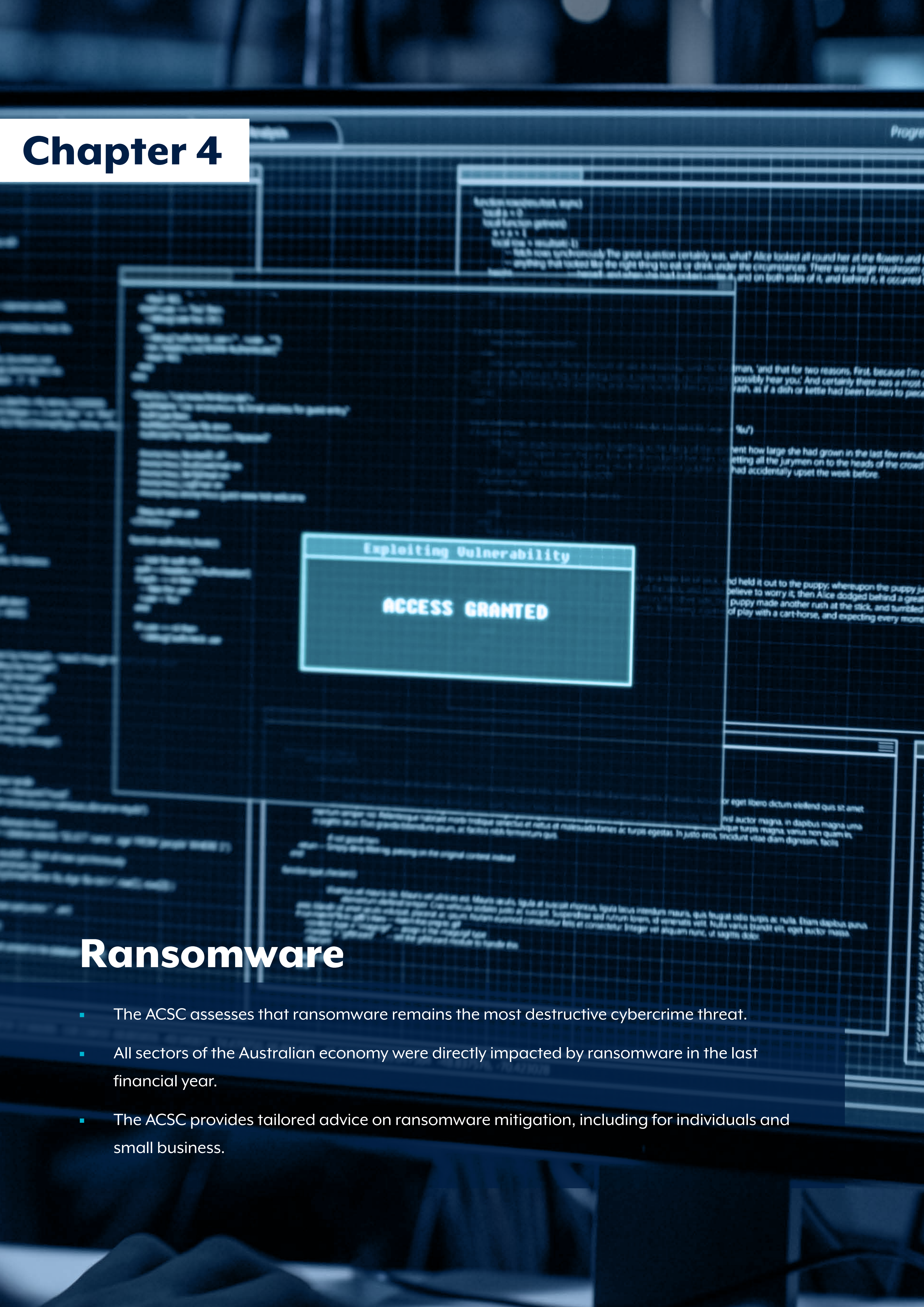
March 2022
Backups
ACSC Alert and Advisory

April 2022
Ransomware

May 2022
Password Managers

June 2022
Email Security

Chapter 4



Ransomware

- The ACSC assesses that ransomware remains the most destructive cybercrime threat.
- All sectors of the Australian economy were directly impacted by ransomware in the last financial year.
- The ACSC provides tailored advice on ransomware mitigation, including for individuals and small business.

Ransomware targeting

Ransomware is a cyber dependent crime which can impact everyone from consumers through to countries. For example, the Costa Rican government declared a state of emergency in May 2022 following ransomware attacks on nearly 30 government institutions, including its health, finance, energy and social services departments. While Australia has not experienced an incident of this scale, the potential remains for cybercriminals to cause widespread disruption.

Top-tier ransomware groups are continuing to target Australian 'big game' entities—organisations that are high profile, high value, or provide critical services. While global trends indicate a decline in 'big game' targeting and a shift towards targeting small and medium sized businesses, that change has yet to be seen in Australia.

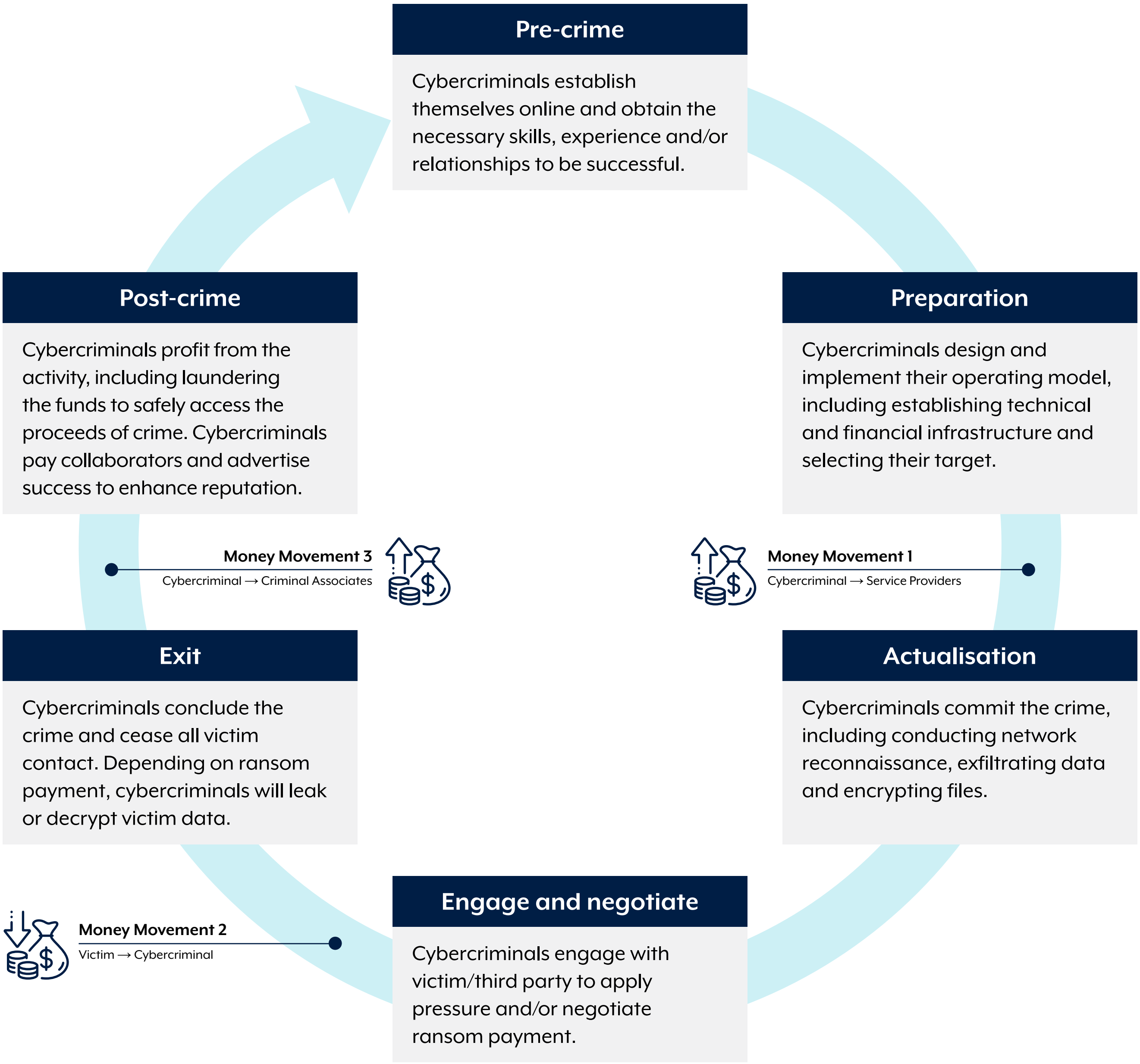
The business model of ransomware groups continued to evolve. Some ransomware groups now share victim information, increasing the ransomware threat as victims potentially face targeting by more than one group. For example, after announcing its shutdown, the BlackMatter group transferred its victims to ransomware infrastructure owned by another group, known as Lockbit 2.0. And, in October 2021, members of the Conti ransomware group reportedly began selling access to victims' networks, enabling follow-on targeting by other actors.

Ransomware tactics

The combination of data encryption and threats to publicly release sensitive information as a method of pressuring ransomware victims into paying is known as 'double extortion'. Victims who previously would have been able to recover from a ransomware incident by maintaining regular backups may still be vulnerable to reputational damage resulting from double extortion. In 2021–22, ransomware actors continued to incorporate additional extortion tactics in their operations to more effectively extract payment from victims. This is often referred to as 'multifaceted extortion'. Examples of additional extortion tactics include convincing third-party stakeholders to pressure victims into negotiation, and sustained DDoS attacks against the victim's network during ransom negotiations.

Ransomware-as-a-Service

The ACSC observed the emergence of new and possibly rebranded RaaS operations over 2021–22. The availability of RaaS offerings affords cybercriminals a choice about the tools they can use. Ransomware syndicates also continued to professionalise by using third parties to negotiate with victims, assist them in receiving their ransom payments, and arbitrating disputes between actors.



Pre-crime

Cybercriminals establish themselves online and obtain the necessary skills, experience and/or relationships to be successful.

Preparation

Cybercriminals design and implement their operating model, including establishing technical and financial infrastructure and selecting their target.

Money Movement 1

Cybercriminal → Service Providers

Actualisation

Cybercriminals commit the crime, including conducting network reconnaissance, exfiltrating data and encrypting files.

Engage and negotiate

Cybercriminals engage with victim/third party to apply pressure and/or negotiate ransom payment.

Money Movement 2

Victim → Cybercriminal

Exit

Cybercriminals conclude the crime and cease all victim contact. Depending on ransom payment, cybercriminals will leak or decrypt victim data.

Money Movement 3

Cybercriminal → Criminal Associates

Post-crime

Cybercriminals profit from the activity, including laundering the funds to safely access the proceeds of crime. Cybercriminals pay collaborators and advertise success to enhance reputation.

Figure 10: The ransomware business model

Ransomware trends

All sectors of the Australian economy were directly impacted by ransomware in 2021–22. The ACSC received 447 ransomware cybercrime reports via ReportCyber. While this is a 10 per cent decrease compared with the 2020–21 financial year, reports remain higher than in 2019–20. It is also likely that ransomware remains significantly underreported, especially by victims who choose to pay a ransom.

The education and training sector reported the most ransomware incidents in 2021–22, rising from the fourth-highest reporting sector in 2020–21. The threat to the education and training sector is significant as its business model favours open collaborative environments. Remote learning during the coronavirus pandemic also introduced large numbers of personal devices and new software into this sector.

The top 5 reporting sectors for ransomware accounted for 47 per cent of all ransomware-related cybercrime reported to ReportCyber during the 2021–22 financial year.

The ACSC responded to 135 cyber security incidents related to ransomware, an increase of over 75 per cent compared to 2019–20. In addition, the ACSC identified and notified 148 organisations of ransomware activity.

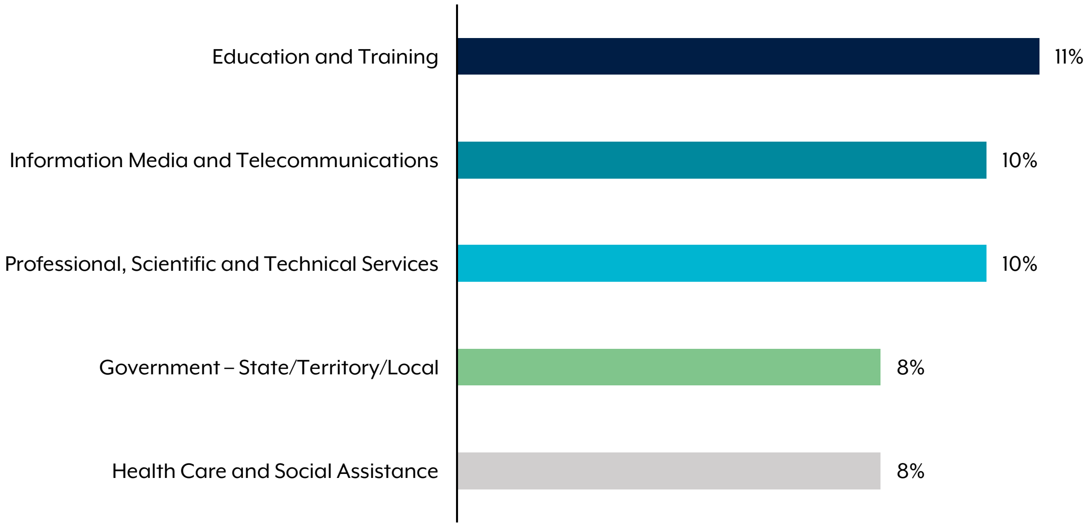


Figure 11: Top 5 reporting sectors for ransomware-related cyber security incidents

AFP–ACSC–ACIC Initiative: Operation Orcus

In July 2021, the AFP established Operation Orcus, an AFP-led multi-agency taskforce to coordinate law enforcement efforts against ransomware, particularly targeting ransomware developers and those who use RaaS. The taskforce comprises AFP, ACSC, ACIC, AUSTRAC and state and territory police. Operation Orcus also works with international partners, including Interpol and Europol.

During 2021–22, Operation Orcus analysed hundreds of ransomware incidents and prepared and distributed intelligence reports. Operation Orcus detected indicators of compromise showing Australian organisations being targeted by ransomware, and notified impending victims. These notifications prevented attacks and protected Australian organisations from financial loss.

Data breaches

Cybercriminals target the PII of employees and customers, seeking to maximise the commercial and reputational impact of a data breach. In the last financial year, human resources organisations such as payroll and recruitment companies have been frequently targeted by ransomware actors, as these types of companies provide services across a wide range of sectors. Compromises of payroll providers in 2021–22 led to the data of hundreds of thousands of Australian employees being accessed and exposed.

Social assistance organisations, which hold sensitive data on vulnerable people, have also been targeted in Australia and internationally. For example, in January 2022, the Swiss-based International Committee of the Red Cross publicly stated a ransomware attack on its servers had compromised the personal data of more than half a million people, including refugees and internally displaced people in conflict zones across the world.

Case Study: Australian social assistance organisation

In March 2022, an Australian social assistance organisation was targeted by ransomware resulting in the theft of data. The malicious actor gained access to the organisation's servers through exploiting an unpatched version of Microsoft Exchange. Within 4 days, the malicious actor moved from initial access to encryption. The organisation's Chief Information Security Officer told the ACSC, "it spins my head about how quickly they were able to move around the network".

The organisation identified that its systems had been encrypted and immediately notified Commonwealth and state agencies. It engaged its existing commercial incident response provider to provide technical support and conduct an investigation. The organisation credits its ability to recover so quickly to maintaining a strong relationship with their incident response provider and moving to cloud-based backups in the months before the incident. Remediation and related network security improvements cost approximately $200,000, which was substantially less than the ransom demanded.

Since this incident, the organisation continues to monitor for residual risk, and is hardening its cyber defences more broadly, including enhanced restrictions for applications, and better managed network awareness.

During the organisation's engagement with the ACSC, it shared indicators of compromise, which the ACSC shared through the CTIS portal. This enabled other organisations to better protect themselves, ultimately strengthening the security of Australian organisations.

Cost to victims of ransomware

Regardless of the size of the victim, ransomware can be expensive to resolve. The most immediate costs come from the lost productivity due to system downtime, and the time and money needed to rebuild systems following an incident. The legacy of a ransomware incident poses additional challenges, such as tarnishing a victim's reputation among its customers.

Case Study: Australian healthcare organisation

A Sodinokibi (also known as REvil) ransomware group targeted a medium-sized business in the Australian healthcare sector, encrypting critical files and preventing access to business-critical systems. The malicious actor demanded several hundred-thousand dollars in exchange for the decryption keys and an assurance that the stolen data would not be publicly released.

Even with the involvement of specialists, ransomware incidents can take months to resolve. In this instance, despite the engagement of a law firm, third-party negotiator and insurance company, and a willingness by the victim to pay the ransom, resolution and restoration of data took approximately 3 months, severely impacting business operations for the victim.

Victims of ransomware attacks continued to use third-party negotiators to facilitate payment of ransom demands in 2021–22. The level of coverage provided under cyber insurance policies is also a contributing factor in how these incidents are handled and resolved by victims, and whether a business decides to pay the ransom.

A 2022 study published by the Australian Institute of Criminology found only 19 per cent of ransomware victims sought advice or support from police or the ACSC. However, the study found nearly 60 per cent sought help from at least one formal source outside of their family or friends. The study found 23.2 per cent of small to medium business victims paid the ransom, with many millions of dollars being paid in ransoms and other associated costs.

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 or sale of any stolen data. 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. This is essential to develop national visibility of ransomware threats, including emerging trends and ransomware precursors. Even when organisations have sufficient in-house or contracted incident response to address a ransomware incident, sharing technical and contextual information with the ACSC enables the ACSC to implement measures to reduce ransomware targeting and protect other potential victims.

Ransomware Action Plan

On 13 October 2021, Australia's Ransomware Action Plan was released. The plan outlined the proposed capabilities and powers that Australia would use to combat ransomware, and a suite of reforms designed to help the Australian Government better assist victims of ransomware attacks and prosecute ransomware groups. Complementing a range of measures under the 2020 Cyber Security Strategy, the plan seeks to ensure that Australia remains a hard target for cybercrime by launching additional operational activity to target criminals seeking to disrupt, and profit from, Australian business and individuals.

What you should do

How to protect yourself from ransomware

To support Australians in preventing and mitigating ransomware incidents, the ACSC provides technical advice and guidance, including profiles of ransomware actors, via cyber.gov.au. The ACSC also collaborates with domestic and international intelligence and law enforcement partners to disrupt the syndicates causing the greatest harm, and provide operational intelligence regarding cybercriminals targeting Australia. This is a part of a whole-of-government approach to combating ransomware.

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.

Government, large businesses and critical infrastructure:

- Implement the ACSC's Essential Eight Mitigation Strategies and Strategies to Mitigate Cyber Security Incidents.
- Become an ACSC partner and participate in ACSC initiatives and exercises.

Chapter 5

Critical infrastructure

- The disruption of critical infrastructure puts access to essential services at risk.
- Globally, critical infrastructure has been increasingly targeted by malicious actors.

Current critical infrastructure threat

The cyber threat to Australia's critical infrastructure is an enduring concern, because the social or economic well-being of the nation depends on critical infrastructure assets working in cohesion. Critical infrastructure encompasses the physical facilities, communication networks, and information and operational technologies that provide essential services. A sustained disruption in one part of the critical infrastructure ecosystem has knock-on effects elsewhere in the economy, and could ultimately lead to harm or loss of life, as seen internationally as a consequence of ransomware attacks on health services. The potential remains for state actors and cybercriminals to cause similar disruption through targeting of Australian critical infrastructure entities.

During 2021–22, critical infrastructure networks globally were targeted at phenomenal rates. Russia's targeting of Ukrainian critical infrastructure was particularly prolific, including the use of destructive malware against high-voltage electrical substations. However, the threat is not limited to Ukraine. Some Russia-aligned cybercrime groups—including one that has successfully targeted Australian critical infrastructure—have publicly threatened to conduct operations against Ukraine's allies.

The risk to Australia's critical infrastructure networks is real. In 2021, the corporate network of electricity generator CS Energy was targeted by the Russia-aligned Conti ransomware group, as detailed below.

Case Study: CS Energy

In 2021, the corporate ICT network of Queensland Government-owned electricity generator CS Energy —which generates 10 per cent of the electricity for the national electricity market— was targeted by the Conti ransomware group. On 27 November 2021, CS Energy became aware of a ransomware incident affecting its corporate network and immediately severed the external internet connection to its corporate network and initiated business continuity procedures.

CS Energy also alerted relevant Australian Government and Queensland Government agencies, and as an established ACSC partner, closely collaborated with ACSC incident response support and external specialists to remedy the incident. As a result of network segregation —a recommended mitigation for business continuity— CS Energy's operational technology systems were physically segregated from the corporate network, ensuring that the incident did not compromise operational technology systems, including electricity generation. Energy supplies were not affected by the incident.

This incident highlights the value of network segmentation and the importance of having incident response, business continuity and disaster recovery plans in place. By acting decisively, CS Energy, commercial incident response and cyber security specialists, and the ACSC worked together to respond to the incident, demonstrating the maturity of Australia's cyber security sector.

Not all targeting of critical infrastructure is geostrategic; some is profit-motivated, and some is opportunistic exploitation of widespread vulnerabilities. Even the most trivial exploitation can result in major impact, especially if malicious actors move laterally from internet-facing devices on corporate networks to the operational networks of critical infrastructure providers. Certain critical infrastructure networks face additional challenges, such as the use of legacy operational technology with long life cycles (up to 50 years for some operational hardware), making patching and monitoring of networks more difficult.

Critical infrastructure trends

During 2021–22, the ACSC reshaped its definition of critical infrastructure to better align with the definitions of Regulated Critical Infrastructure and Systems of National Significance under the SoCI Act. In the 2020–21 financial year, the ACSC defined approximately one quarter of cyber security incidents it responded to as affecting critical infrastructure. However, this definition covered a range of infrastructure and services outside the scope of the SoCI Act, and also captured some severe incidents regardless of sector. In the 2021–22 financial year, using the new definitions, 95 cyber incidents (approximately 8 per cent of all cyber incidents the ACSC responded to) affected critical infrastructure. Since the implementation in April 2022 of amendments to the SoCI Act, the ACSC has notified 5 critical infrastructure entities of cyber incidents and vulnerabilities on their networks.

The ACSC urges organisations to report all cyber security incidents, regardless of whether or not their organisation is subject to mandatory reporting under the SoCI Act. Reporting increases the visibility of threats, enables the identification of trends, and supports the prevention and mitigation of future incidents.

Ransomware and critical infrastructure

Over 2021–22, there were further examples of ransomware groups targeting critical infrastructure. For instance, the BlackCat ransomware group targeted government and critical infrastructure organisations, as well as the finance and construction sectors globally.

The threat to critical infrastructure is not limited to large utilities such as electricity providers. For example, local governments can be an attractive target, as some councils have responsibility for essential services such as water and sewage.

Case Study: Local council ransomware incident

In April 2022, a NSW council was targeted by a ransomware incident. The initial access occurred at least 2 weeks before the incident, with the malicious actor likely timing the incident to occur over the Easter long weekend.

Manual processes were immediately implemented to manage water-quality testing and level monitoring, and temporary servers were established within 24 hours to restore remote monitoring.

The incident impacted a wide range of business operations, including council minutes, employee financial data, and systems responsible for monitoring water quality. The incident also had a huge impact on council technology staff, who worked 40–80 hours overtime a week during their initial response.

The council engaged a commercial incident response provider, and its Managed Service Providers (MSP) deployed additional capabilities. The ACSC provided advice to the council and warned ACSC partners in the water sector to be alert to possible ransomware targeting.

The incident demonstrates the interplay between IT, operational technology, and the physical environment. The initial access through a legacy entry point impacted multiple systems, including operational technology systems, which meant that council workers had to manually test water quality and levels following overnight rain. A swift response by the council, its MSP, and the ACSC ensured there was no compromise of water or sewage services. The council's MSP continues to monitor the darkweb for data leaks.

The case study demonstrates the importance of decommissioning legacy systems and erecting firewalls between IT and operational technology systems.

Advice and support for critical infrastructure organisations

A wide range of critical infrastructure providers are subject to mandatory cyber incident reporting requirements, including critical food, transport and higher education assets. The ACSC has a dedicated portal for reporting cyber security incidents that impact critical infrastructure assets, including a list of critical infrastructure sectors and asset classes following amendments to the SoCI Act.

In recognition of the additional cyber security obligations critical infrastructure organisations have, the ACSC offers tailored critical infrastructure exercise and uplift programs. These assist ACSC partners to implement risk mitigation strategies.

ACSC initiative: AquaEx

In August 2021, the ACSC coordinated a national cyber security exercise series in partnership with Australia's urban water and wastewater sector and government agencies. The exercise series provided an opportunity for industry and government to exercise arrangements for responding to, and recovering from, a ransomware incident impacting Australia's urban water and wastewater sector.

Planning for the exercise series included exercise management workshops and cyber security information sessions. These provided opportunities for participants to share approaches to preventing, detecting and responding to ransomware incidents.

Executive and senior management were actively engaged in the exercise series, with some organisations conducting their largest ever exercises. Participating executives have indicated that they would like their organisation to be involved in more exercises like AquaEx in the future. It is this level of support and engagement at senior levels that will continue to increase organisational cyber resilience.

Opportunities that have been identified as a result of AquaEx include organisations continuing to review and exercise their cyber response plans, expanding their playbooks to include more threat vectors, and solidifying the relationships developed between industry and government.

Despite COVID-19 impacts, the exercise reached over 750 participants from across industry and government who were able to work together to strengthen cyber resilience across the nation.

ACSC initiative: Critical Infrastructure – Uplift Program

In support of Australia's critical infrastructure, in 2021–22 the ACSC piloted the Critical Infrastructure Uplift Program (CI-UP). CI-UP is a voluntary service provided by the ACSC to help protect Australia's essential services from cyber threats by raising the cyber security levels of critical infrastructure organisations.

Through close collaboration between the ACSC and partners, CI-UP evaluates the cyber security maturity of critical infrastructure and systems of national significance. A combination of Cyber Security Capability and Maturity Model (C2M2) and Essential Eight maturity models are used to deliver prioritised vulnerability and risk management strategies.

The pilot concluded in June 2022. The ACSC now provides 2 models for CI-UP service:

CI-UP: A modular suite of cyber security maturity activities undertaken through close collaboration with the ACSC to deliver holistic cyber security maturity uplift for CI-UP partners.

CI-UP (Self-Assessment): A self-assessment C2M2 evaluation tool enabling ACSC partners to access online resources through the ACSC Partner Portal.

Case Study: CI-UP pilot uplift

In late 2021, the ACSC undertook multiple pilot uplifts with critical infrastructure organisations at differing cyber security maturity levels.

In one pilot, the ACSC partnered with Queensland Airports Limited (QAL) to understand the maturity of its cyber security. This uplift was conducted remotely due to COVID-19 impacts, but was successful nonetheless due to QAL's proactive engagement. The active participation gave the CI-UP team a deep understanding of QAL's baseline cyber security posture, enabling the provision of targeted advice.

Despite the challenges of working during COVID-19 restrictions, the ACSC and QAL teams collaborated to deliver one of QAL's most successful cyber outcomes to date.

As a result, QAL has a better understanding of its holistic cyber security posture, and a prioritised list of recommended remediation activities to continue hardening its cyber defences.

Chapter 6

Critical vulnerabilities

- The ACSC observed an increasing trend of state actors and cybercriminals rapidly exploiting publicly reported critical security vulnerabilities.
- Rapid and comprehensive patching is vital, along with constant monitoring for indicators of compromise.

Vulnerabilities being targeted faster and by more actors

During 2021–22, the number of software vulnerabilities recorded worldwide increased by more than 25 per cent compared to the previous financial year. Over 24,000 Common Vulnerabilities and Exposures (CVEs)were identified during 2021–22. Of these, there were numerous critical and high-impact vulnerabilities, with notable examples including vulnerabilities in Microsoft Azure and Log4j products. Within hours of disclosure, the ACSC identified malicious actors conducting scanning and reconnaissance against internet-accessible networks to identify unpatched software. In some instances, cyber actors successfully compromised Australian networks using publicly disclosed critical vulnerabilities.

The rapid use of newly released critical vulnerabilities is now standard tradecraft for many malicious actors. Certain software and hardware is used ubiquitously across government, critical infrastructure, small business and by individual users, presenting malicious actors with a plethora of potential victim networks. When a new vulnerability emerges, the ACSC's Cyber Hygiene Improvement Programs (CHIPs) frequently identifies numerous Australian devices which are unpatched and vulnerable to exploitation.

ACSC Initiative: Cyber Hygiene Improvement Programs (CHIPs)

CHIPs is an ACSC capability that tracks and monitors the cyber security posture of Australian, state, territory and local government entities' internet-facing assets. CHIPs also conduct rapid operational tasking when potential cyber threats emerge, such as newly disclosed vulnerabilities.

Through these activities, CHIPs can quickly build visibility of security vulnerabilities across all levels of government and provide vulnerability notifications to system owners.

In 2021–22, 49 high priority operational tasks were undertaken to protect Australian networks, including scans of government entities and Australian-attributed Internet Protocol addresses for potential compromise by critical vulnerabilities.

Case Study: Australian energy provider

Following the public disclosure of a vulnerability in April 2022, CHIPs contacted several Australian organisations from across the government, critical infrastructure, transportation and services sectors, notifying them of potentially vulnerable software on their internet-facing servers, and offering assistance. One of the organisations contacted was an Australian energy provider.

Immediate actions from the energy provider in response to ACSC's notification confirmed 2 servers had been exploited. Existing network segmentation, specifically a demilitarised zone (DMZ)—a network kept separate from the core network to protect information from less trusted networks, such as the internet—worked as intended. As a result, energy operations were not disrupted. The provider was quick to remediate by restoring the affected servers from backups and applying relevant patches.

Further to the actions of the energy provider, the ACSC conducted a forensics investigation to reconstruct the steps taken by the malicious actors. The investigation found that multiple instances of successful exploitation of the vulnerability occurred in a very short period of time. Evidence suggests that exploitation was conducted by multiple actors, including state-sponsored and criminal entities, much of which was likely automated. Sophisticated actors sought to access user login data, with the likely intent to gain more persistent access once the compromise was remediated.

The responsiveness of the energy provider and strong network segmentation were crucial to containing the compromise.

Comparative critical vulnerabilities timelines

The time between vulnerability disclosure and exploit is closing rapidly; what once took weeks is now taking days or even hours. The following timelines highlight the shortening window for organisations to mitigate threats:

F5 BIG-IP

What is F5 BIG-IP?

A platform used to control traffic that passes through an enterprise network, developed by US company F5.

4 May 2022

F5 publicly disclosed a vulnerability in BIG-IP network devices that allowed malicious actors to execute arbitrary commands, create or delete files, or disable services. F5 encouraged users running at-risk versions to upgrade as soon as possible.

6 May 2022

ACSC performed CHIPs scanning to determine how many Australian devices were vulnerable, and notified government operators.

Confluence

What is Confluence?

A web-based database tool for team collaboration, developed by Australian technology company Atlassian.

25 August 2021

Atlassian publicly announced a vulnerability (CVE-2021–26084) in certain versions of Atlassian Confluence and released software version updates the same day.

The scalability and low cost of automated cyber exploitation techniques mean the driver for this type of compromise is likely to be the existence of vulnerabilities in victim organisations, rather than an adversary's interest in a particular network. This ability of a wide array of cyber threat actors to compromise multiple networks, and then assess the value of those accesses, will make it more difficult to attribute a specific motive for targeting an individual Australian network.

Key takeaway

In an environment where multiple vulnerabilities are disclosed, rapid patching is not enough. Organisations must also monitor for indicators of compromise.

3 **Days from proof of concept until reported exploitation**

6-7 May 2022

Just days after the vulnerability was disclosed, **researchers published exploits, with malicious actors soon using them in attacks** across the internet.

9 May 2022

The ACSC published an Advisory addressing multiple vulnerabilities in the F5 BIG-IP Product Range.

Exploits which required just 2 commands and some headers became publicly known. The vulnerability was so easy to exploit that some security researchers speculated that it did not end up in the products by accident.

10 May 2022

Security researchers tweeted that “real world devices are being erased”. **The ACSC received its first reported Australian incidents relating to exploitation of F5.**

31 August 2021

A Proof of Concept for the exploit was published online; first public reports of exploitation occurred the same day.

1 **Day from proof of concept until reported exploitation**

1 September 2021

A CHIPs scan detected malicious actors scanning for, and attempting to exploit, this vulnerability on Australian networks. The ACSC published an Advisory the same day.

Key takeaway

Over two-thirds of the cyber security incidents the ACSC responded to relating to this vulnerability occurred in the first 6 days following the Proof of Concept, underscoring how new vulnerabilities are being rapidly exploited by malicious actors.

Log4j

The most prevalent critical vulnerability in the 2021–22 financial year was Log4j. Log4j is a popular software building block found in a wide variety of Java applications. It provides logging functionality, recording the activity of the software in order to diagnose problems. Over 100,000 products may contain Log4j—as Log4j is open source software, there is no definitive list.

The series of Log4j vulnerabilities made public in December 2021 were trivial to exploit. The vulnerability could be used to execute code on the servers of the Minecraft video game by pasting messages into a chat box, for example.

In response to the Log4j vulnerabilities, the ACSC raised awareness, provided timely advice, and worked closely with government, industry partners and impacted organisations to protect against exploitation of this vulnerability. Over December 2021 – January 2022, the ACSC provided technical support to impacted organisations, released 2 critical Alerts and 2 Advisories that were regularly updated, hosted 7 information sharing events through the ACSC Partnership Program, and amplified advice on social media which had a potential reach of over one million people.

The ACSC is aware of malicious actors, including sophisticated cyber threat actors, conducting a large number of reconnaissance scans for Log4j vulnerabilities. Some Australian networks were compromised through Log4j, and the ACSC responded to over 50 cyber security incidents.

The ACSC has identified Log4j exploits being used months after the initial disclosure. Malicious actors also routinely scan for vulnerabilities years after they are initially disclosed, targeting networks which are running legacy software or have failed to patch. For instance, a 28 April 2022 Joint Five-Eyes Advisory observed that 6 of the top 15 Routinely Exploited Vulnerabilities in 2021 were first disclosed in 2020 or earlier. Log4j is likely to be a means of access for malicious actors for years to come.

Log4j Timeline

24 November 2021

The cloud security team of Chinese company Alibaba privately reported the Log4j vulnerability to the software developer.

10 December 2021

The vulnerability was publicly disclosed by cyber security researchers. The ACSC issued a public Alert the same day and commenced a comprehensive suite of awareness and response initiatives to prevent potential compromises.

13 December 2021

The ACSC commenced technical incident response assistance to impacted organisations, and commenced briefings of the National Cyber Security Committee, Australian Government Chief Information Officers and industry partners.

What you should do

Patching and uplifting networks

In the face of increasingly rapid critical vulnerabilities, applying patches to applications and operating systems has become even more essential. Once a security vulnerability in an internet-facing service is made public, it can be expected that malicious code will be developed by adversaries within 48 hours. There are cases in which adversaries have developed malicious code within hours of newly discovered security vulnerabilities. The ACSC therefore recommends patching internet-facing services within 48 hours if an exploit exists. More detailed advice is available in the ACSC publication Assessing Security Vulnerabilities and Applying Patches.

Some sectors of the Australian economy have lagged in their patching rates. A limited analysis of patching rates following the 2021 Microsoft Exchange vulnerabilities, for instance, indicated that the Professional, Scientific and Technical Services sector had the highest number of unpatched Microsoft Exchange servers overall, with a rate of unpatched servers significantly higher than its share of the economy by number of businesses. This sector includes industries such as legal and accounting services, which hold significant volumes of personal information on clients.

In addition to rapid patching, organisations need to monitor for Indicators of Compromise, as compromise may have already occurred before the release or application of patches. This is especially so for zero-day exploits—vulnerabilities which have been exploited before becoming publicly known. For instance, Log4j was first exploited at least 10 days before being publicly disclosed.

It is vital that patching is comprehensive, and legacy assets are accounted for. Many organisations struggle to maintain an accurate inventory of their ICT assets, and malicious actors know that the easiest path to a target network is often through unknown or abandoned ICT assets. The ACSC recognises that some sectors have unique requirements, such as legacy operational technology, and offers tailored uplift advice for such sectors.

14 December 2021

The ACSC published an updated Alert advising the ACSC had observed active exploitation of this vulnerability within Australia.

15 December 2021

The ACSC published a public technical Advisory.

16–22 December 2021

The ACSC published additional Alerts and Advisories, and public webinars.

23 December 2021

The ACSC published an additional Alert, highlighting malicious actors using Log4j for ransomware activities.

Chapter 7

Cyber defence and resilience

- Malicious actors are exploiting Australians' desire for interconnected digital services.
- Organisations can improve their cyber posture through implementing the Essential Eight.
- Individuals should employ automatic updates and replace obsolete software and hardware.

Interconnectivity brings risks and opportunities

The virtualisation of Australian life that accelerated during the coronavirus pandemic has become entrenched. Remote working arrangements have given way to a hybrid working model, further increasing cyber security risks as employees switch regularly between personal and corporate devices.

For example, small office/home office (SOHO) modems, routers and network-attached storage are usually insecurely designed with minimal security maintenance. SOHO routers are notorious for having insecure firmware, hardcoded backdoors, and inconsistent patching. Even if secure patches are available, individual users are highly unlikely to install them. And most SOHO routers manufactured before 2017 have no ability to automatically update firmware. Meanwhile, the Internet of Things is growing by billions of devices each year and will introduce new types of vulnerabilities—for instance, in April 2022, researchers released a proof of concept for compromising smart speakers by having the device issue voice commands to itself.

The blurring of work and home lives has made the information held by individuals more valuable to malicious actors. Email accounts listed in PII holdings will almost certainly be under increased threat of spear phishing activity. The theft of PII creates a risk that ordinary Australians will be victimised and need substantial support. In some cases, a victim will be impacted for the rest of their life as exposure of their personal information, once leaked or sold, cannot necessarily be remediated.

As interconnectivity grows, malicious actors are increasingly looking to compromise multiple victims across a range of sectors via a single entry point. The ACSC expects this trend to continue. For example, MSPs were targeted over 2021–22 as they are used by government, commercial and not-for-profit businesses of all sizes, making them an attractive target for malicious actors. Malicious actors increasingly view the supply chain as a priority target and a vector for compromise.

Case Study: Kaseya supply chain ransomware attack

In July 2021, US ICT management provider Kaseya became the victim of a sophisticated ransomware cyberattack, which exploited a vulnerability in remote management software. This allowed the ransomware affiliate to carry out a supply chain compromise of Kaseya's customers. The cybercriminal group responsible demanded USD 70 million in Bitcoin for a universal decryption key that would unlock customer data.

Kaseya responded by advising on-premises customers to shut down affected servers, and subsequently released a compromise detection tool and software patches to customers. The company also warned of spammers exploiting the incident by sending phishing emails that had fake notifications with malicious links.

Due to Kaseya's swift response, the attack was contained to fewer than 60 MSPs of its more than 37,000 customers worldwide, and between 800 and 1500 downstream customers, including 3 affected MSPs in Australia.

From 4 to 5 July 2021, the ACSC responded to a small number of cyber security incidents involving Australian entities affected by the Kaseya software compromise, including businesses in the Education, Health, and Professional, Scientific and Technical Services sectors. The ACSC also published an Advisory on the Kaseya ransomware attack.

On 22 July 2021, Kaseya obtained a universal decryption key to unlock its files and those of its customers, which allowed Kaseya to restore functionality to all of its clients. Kaseya has stated publicly that it did not pay a ransom to the cybercrime affiliate responsible for the attack. While interconnectivity introduces new risks, it also presents opportunities. Workplaces have become more resilient through remote working arrangements and greater use of cloud services, reducing the risk of single points of failure within in-house networks. Improved interconnectivity between government and industry is allowing real-time sharing of threat intelligence, enabling organisations such as financial institutions to better protect PII.

What is the ACSC doing?

The ACSC is delivering a range of initiatives that streamline—and where possible, automate—active cyber defence and intelligence sharing. REDSPICE will further strengthen Australia's cyber defences.

ACSC initiative: CTIS

The CTIS service enables the sharing of cyber threat intelligence at machine speed. Through the use of automation, participating entities receive cyber threat intelligence in a structured and timely manner.

The CTIS Data Model enables partners to share cyber threat intelligence through a common language and outlines standards to share data in alignment to the 5 Cs: Content, Context, Clarity, Communication and Confidence.

On 1 November 2021, the bi-directional CTIS platform went live.

On 19 November 2021, the ACSC facilitated the first successful bi-directional share between a commercial entity (National Australia Bank - NAB) and a Government department. Cyber Threat Intelligence shared by members via CTIS is made available to other members in order to support the identification of malicious cyber activity in their environments. In one instance, intelligence shared by NAB provided the means to identify suspicious cyber activity in an environment that ACSC previously had no visibility of.

25,341

indicators have been provided by the ACSC, including from victims who are not ACSC Partners.

741

have been provided by CTIS analysts working for ACSC's delivery partner, Deloitte.

2,261

have been shared with CTIS by ACSC Partners.

Following an early release to a sample-set of partners, CTIS was released broadly to ACSC network partners in June 2022.

ACSC initiative: Australian Protective Domain Name System

The Australian Protective Domain Name System (AUPDNS) is dedicated to protecting government networks. The system uses verified threat intelligence to build a 'block list' of known malicious web domains.

Providing protection against malware, spyware phishing attacks, viruses, and malicious sites, AUPDNS monitors connections between an organisation's network and the internet. AUPDNS also stops malware already on devices from 'calling home', mitigating the damage from an attack. The information captured within AUPDNS also helps build the ACSC's cyber threat picture.

In the 2021–22 financial year, AUPDNS processed more than 36 billion queries, and blocked over 24 million domain requests. AUPDNS onboarded 171 organisations, including a number of state and local government agencies.

ACSC initiative: Domain Takedown Service

In response to the increasing threat posed by domains hosting malicious software, the ACSC launched the Domain Takedown Service pilot in 2021.

Upon detecting suspected malicious software, the service verifies maliciousness before issuing a takedown notification request to the relevant Domain Host. The service also operates 10 'honeypot' servers on Australian IP ranges, giving the ACSC the ability to directly report malicious domains for manual verification and takedown. The service only targets those attack types which fall under ASD's cyber security function as per the *Intelligence Services Act 2001*.

In 2021–22, the service focused on 4 lines of effort:

Line of effort	Number of notifications issued	Number of takedowns	Targeting success Rate
Government (Australian, state & territory, local)	1,352	1,333	99%
Australian vaccine rollout	16,291	15,932	98%
Flubot text message malware	19,117	19,117	100%
Brute force attacks against Australian servers	29,446	29,278	99%

Uplifting an interconnected Australian economy

Australia's best defence in a rapidly evolving cyber threat environment is to build resilience across businesses and organisations, and among individuals. As vulnerabilities and interdependencies increase, preventative cyber security measures are not sufficient; organisations should also develop and test incident response, business continuity and disaster recovery plans. Commercial incident response providers have a particularly important role to play; they offer services to organisations which may have limited in-house capabilities, as well as reduce demand on the ACSC's finite incident response capabilities. The ACSC is conducting a suite of incident response transformation activities to increase information sharing and reporting, while growing the scale and maturity of commercial providers and the cyber security sector as a whole.

The consequences for organisations which fail to manage cyber security incidents are clear. In May 2022, the Federal Court of Australia found that financial planning firm RI Advice had breached its financial services license obligations by having inadequate cybersecurity risk management systems. While the judgement does not set a legal standard for Australian Financial Services Licencees or other organisations, it is a strong reminder that company boards should consider cyber resilience as part of their statutory responsibilities. The ACSC publishes tailored advice for company boards, such as the January 2022 publication Log4j: What Boards and Directors Need to Know. The ACSC also directly engages senior executives through the Joint Cyber Security Centres.

Case Study: Qantas

Qantas and the ACSC have been sharing knowledge for over 12 years. In 2015, Qantas was part of the Prime Minister's Incident Response Taskforce and has participated in multiple other exercises. The ACSC and Qantas now have information exchange agreements and dedicated liaison personnel.

Qantas regularly checks with the ACSC to verify intelligence gathered from other sources, seeks advice on new and unusual cyber security challenges, and seeks feedback on its incident response processes.

The ACSC also learns from Qantas. Qantas shares insights with ACSC analysts on how threat information and leads are gathered and managed in the private sector. The ACSC, Qantas and other aviation sector partners are also members of the Australian Aviation Cyber Council.

During 2021–22, the benefits of the partnership were demonstrated during Qanta's involvement in the Australian Government's distribution of COVID-19 vaccines. It was in the national interest to ensure that the vaccine distribution process was not interrupted by a cyberattack, and Qantas and the ACSC worked closely to make sure Qantas's cyber protections were fit for the task.

Qantas Group Chief Information Security Officer Jeffrey Choi stated, "My team continues to benefit from sharing knowledge and expertise with the ACSC, as well as through forums with industry peers. ACSC's Advisories and threat intelligence have given the Qantas Group greater visibility of the threat landscape in which we operate".

What can my organisation do?

Essential Eight

The Australian Cyber Security Centre (ACSC) has developed prioritised mitigation strategies—in the form of the Strategies to Mitigate Cyber Security Incidents—to help organisations protect themselves against various cyber threats.

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.

The Essential Eight remains highly relevant, with a major update released in July 2021. In recognition of the degrading cyber threat environment, in March 2022 the Attorney-General's Department mandated the Essential Eight for all non-corporate Commonwealth entities through amendments to the Protective Security Policy Framework.

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 3 tiers to reach the entire Australian economy:

- **Network Partners** – for organisations with responsibility for their own ICT environments, experts in cyber security such as academics, and not-for-profit institutions. The community of ACSC Network Partners includes cyber security professionals across government, industry, and academia. Bringing together the situational awareness, technical expertise and experience of this community allows the collective public and private sectors to support and learn from each other. ACSC Network Partners are provided access to threat intelligence, news and advice to enhance situational awareness; collaboration opportunities with fellow cyber security professionals and resilience-building activities (such as exercises, discussions, workshops).
- **Business Partners** – for businesses that would like to be kept up to date with relevant cyber security information for their businesses, including those not eligible for the Network Partner tier. This tier of partnership provides organisations with a better understanding of the cyber security landscape and outlines the steps required to protect themselves from cyber security threats. They receive a subscription to the ACSC Alert Service and a monthly newsletter containing news, publications and Advisories produced by the ACSC.
- **Home Partners** – for individuals and families that would like to be kept up to date with relevant information. ACSC Home Partners receive a subscription to the ACSC Alert Service, providing them with a better understanding of the cyber security environment.

Joint Cyber Security Centres

The JCSCs support the Network Partner tier of the ACSC Partnership Program to bring together businesses and the research community, along with sAustralian, state and territory government agencies, in an open and cooperative environment. JCSCs in Adelaide, Brisbane, Melbourne, Perth, Sydney and Hobart, along with a virtual JCSC in Darwin, provide opportunities for the Australian cyber security community to come together in a trusted, neutral environment to drive collaboration and information-sharing.

Over the 2021–22 financial year, ACSC Network Partner membership has increased by 34 per cent, now comprising over 2,300 partners. Business Partners increased by 65 per cent to over 3400 and Home Partners by 8 per cent to over 82,000.

What can individuals do?

The risk of malicious cyber activity impacting Australian individuals remains high. The ACSC provides easy steps to secure your devices and accounts at cyber.gov.au, including step-by-step guides on how to enable multi-factor authentication (MFA) on popular social networking applications.

Individuals are encouraged to patch or mitigate critical vulnerabilities within 48 hours. Individuals should turn on automatic updates on all devices and apps, including personal mobile phones, computers and smart devices such as smart speakers. Individuals should be aware that many device manufacturers and software providers only support updates for a limited number of years, and older devices and software may have security vulnerabilities that cannot be patched.

Individuals should also activate MFA, backup devices, set secure passphrases and be alert for scams.

Individuals interested in becoming an ACSC Home Partner should register for the ACSC Alert Service.

Patch within 48 hours

Turn on automatic updates

For advice, call the

Australian Cyber Security Hotline

1300 CYBER1
(1300 292 371)

Activate MFA, backup devices, set secure passphrases and be alert for scams

Notes

Sources

The ACSC manages or uses a number of unique datasets to produce tailored advice and assistance for Australian Government, organisations and the public. Data used in this report have 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

The ACSC glossary provides definitions for terms used in this Report and other ACSC publications.

Feedback

The ACSC welcomes feedback to improve the services it provides to Australians. Feedback can be provided via our feedback form, by emailing asd.assist@defence.gov.au or by calling 1300 CYBER1 (1300 292 371).