Australian Government

RANSOMWARE ACTION PLAN

Contact us

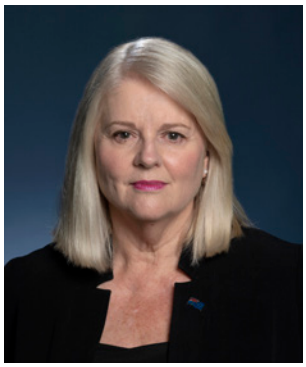
Enquiries regarding the licence and any use of this document are welcome at:

Strategy Division
Department of Home Affairs
4 National Circuit Barton ACT 2600
cybersecuritystrategy@homeaffairs.gov.au

Table of Contents


558.25

Minister's foreword



The Australian Government's cyber security vision is to create a more secure online world for Australians, their businesses and essential services. However, Australia faces a rapidly evolving strategic environment, punctuated by increasing malicious cyber activity conducted by transnational, serious and organised crime groups and individuals. This Ransomware Action Plan sets out the Government's immediate strategic approach to tackle the threat posed by ransomware, and builds on the overarching cyber security architecture instigated in the 2016 and 2020 Cyber Security Strategies, and is designed around the framework of the *National Strategy to Fight Transnational, Serious and Organised Crime.*

We are continuing to observe cybercriminals successfully use ransomware to disrupt services and steal from Australians. Whether it is conducting attacks on critical infrastructure, taking from small businesses or targeting the most vulnerable members of our community, cybercriminals use ransomware to do Australians real and long-lasting harm. In response, the Australian Government is taking concrete action to protect Australians, including working with our international and business partners to combat this global threat.

Criminals are carrying out attacks simultaneously to exploit or steal from as many victims as possible. Over the past 12 months, Australia has faced a 15% increase in ransomware attacks reported to the Australian Cyber Security Centre. During a time where we are focused on growing Australia's future as a modern and leading digital economy, safety, security and trust in the cyber-enabled systems we all rely on has never been of greater importance.

The Ransomware Action Plan takes a decisive stance – the Australian Government does not condone ransom payments being made to cybercriminals. Any ransom payment, small or large, fuels the ransomware business model, putting other Australians at risk. Paying ransoms does not guarantee access to locked systems or sensitive data, and may open the victim up to repeat attacks. We need to ensure that Australia remains an unattractive target for criminals and a hostile place for them to operate.

Recognising that there are several cyber and ransomware initiatives already in place, the ever changing nature of this threat means Australia needs to remain agile and prepared to quickly stand up differing approaches over time. This approach will ensure that Australia can maintain a consistent and mature security posture to meet security objectives well into the future.

Put simply – Australia takes a zero tolerance approach to ransomware.

The Hon Karen Andrews MP
Minister for Home Affairs
October 2021

The threat of ransomware

Ransomware has become an increasingly prevalent global threat, where cybercriminals use readily available software to encrypt electronic devices, folders and files that render systems inaccessible to users. Once files are encrypted, criminals demand a ransom from the system owner in return for the decryption keys, often in the form of hard-to-trace cryptocurrencies. Not only do criminals use ransomware to encrypt files, ransomware also allows criminals to gain access to a network, enabling them to steal sensitive information.

Australia's relative wealth, high levels of online connectivity and increasing delivery of services through online channels make it very attractive and profitable for transnational, organised cybercrime syndicates to target Australians using cyber-enabled tools and techniques. Consistent with global trends, the Australian Cyber Security Centre has continued to observe cybercriminals successfully use ransomware to disrupt operations and cause reputational damage to Australian organisations, and reported a 15% increase in ransomware attacks over the past 12 months.

Globally, it is estimated that there is a ransomware attack on a business every 11 seconds, with ransomware damage losses projected to reach US$20 billion in 2021.[1] Paying a ransom does not guarantee recovery of ransomed data, and only helps promote ransomware as a profitable criminal enterprise.[2] Ransomware and cyber extortion remains the most serious cybercrime threat facing Australia due to its high financial and disruptive impacts to victims and the wider community.

This trend of data theft, encryption, and public shaming reflects an evolution in ransomware tactics to more effectively extort considerable ransoms from victims. Cybercriminals are now regularly exfiltrating data, including customer personally identifiable information (PII), prior to encryption and subsequently threatening to release the stolen information publicly unless the ransom is paid. Victims who would have previously been well prepared for, or able to, recover from a ransomware incident are unlikely to be immune to this tactic known as 'double extortion'. Organisations are now required to evaluate the cost of ransom payment against the potentially severe legal and reputational consequences of a data breach. Other extortion tactics observed in 2020 included committing Distributed Denial of Service to force victims to re-engage in ransom negotiations, directly contacting senior employees (such as Chief Executive Officers or Chief Financial Officers), alerting customers and/or the media to inform them of imminent data leaks, and posting ransom demands directly on victims' publicly facing websites.

In the last 24 months, there has been an increase in number of larger organisations experiencing ransomware. This aligns with global trends and intelligence indicating top tier and highly-skilled cybercriminal groups are moving away from indiscriminately targeting large volumes of small-scale victims and instead tailoring their ransomware campaigns to specific million or billion dollar corporations (referred to as 'big game hunting'). Cybercriminals are exploiting the need for such organisations to maintain effective operation to increase ransom payment.

> ***Globally, it is estimated that there is a ransomware attack on a business every 11 seconds, with ransomware damage losses projected to reach US$20 billion in 2021.***

1. Ransomware: The True Cost to Business, A Global Study on Ransomware Business Impact, Cybereason, June 2021.
2. Locked Out: Tackling Australia's ransomware threat, Cyber Security Industry Advisory Committee, March 2021.

Ransomware attacks typically involve:

- Criminals - perpetrators responsible for the ransomware attack
- Victims - individuals or organisations who have been subject to the ransomware attack
- Facilitators – individuals or companies who may facilitate ransom payments

Types of attacks[3]

Hack and leak	Targeting executives	Tailored ransom demands
After gaining control of a company's IT systems, cybercriminals search for sensitive files, which are stolen before systems can be protected and locked. In the event the ransom is not paid, victims are extorted with threats to publish sensitive information, including on the dark web.	Cybercriminals have started to directly target top executives. The techniques include emailing them directly with threats and ransom demands, as well as gaining access to their inboxes, files and computers and stealing their organisation's data which is then used for extortion or blackmail.	Cybercriminals trawl through stolen data in preparation for ransomware attacks, often demanding a ransom payment that is the same as the insured amount. By insisting on payment in cryptocurrency, the attacker may remain anonymous and free to attack again.

3. Locked Out: Tackling Australia's ransomware threat, Cyber Security Industry Advisory Committee, March 2021.

In May 2021, criminals attacked a United States company, Colonial Pipeline, which carries almost half the fuel supplies that power the east coast of the United States. This ransomware attack resulted in the company's decision to shut down the pipeline. Fuel distribution was disrupted for over a week, during which time the United States experienced fuel shortages, panic buying, and impacts on transport services and air flight schedules.

Criminals have launched ransomware attacks against Australia's critical infrastructure, businesses and members of the community. For example, during the height of the COVID-19 pandemic in 2020, ransomware campaigns targeted Australia's aged care and healthcare sectors. The 'Maze' ransomware encrypted valuable information, such as sensitive personal and medical information, so that it could no longer be used. This reckless activity threatened the operation of health facilities and caused very real health and safety risks to our community. These incidents demonstrate the importance of strong cyber security, particularly in the protection of critical infrastructure.

Case study: Ransomware attacks against the Australian health sector

In early 2019, a specialist unit within a Melbourne hospital was the target of a significant ransomware attack. 15,000 patients' worth of sensitive health information was encrypted and made inaccessible to staff for a duration of three weeks. The perpetrators demanded a ransom be paid in cryptocurrency in exchange for the files to be decrypted and to allow staff to regain access to the information.

It was reported that a payment was made however not all files were recovered.

Assistance is available

Advice on mitigating the threat of ransomware can be found at cyber.gov.au.

If Australian organisations are impacted by ransomware, they can seek assistance from the Australian Cyber Security Centre (ACSC) via 1300 CYBER1. Reporting cyber security incidents enables the ACSC to alert and assist a broader range of organisations, and understand the scope and nature of cyber intrusions.

All Australians can report a cybercrime by visiting cyber.gov.au

Current initiatives to address ransomware

The Australian Government is progressing many lines of effort that combat ransomware, including a $1.67 billion investment over 10 years through *Australia's Cyber Security Strategy 2020* to build new cybersecurity and law enforcement capabilities, protect the essential services upon which we all depend, assist businesses to protect themselves and raise the community's understanding of how to be secure online.

The Government is:

- Strengthening Australia's capability to counter cybercrime through a $164.9 million investment (as part of the $1.67 billion), including $89.9 million to equip the Australian Federal Police with an additional 100 personnel to identify and target cybercriminals;
- Combining the expertise of foreign and domestic law enforcement and intelligence agencies to fight cybercrime through the expanded remit of the Australian Cyber Security Centre within the Australian Signals Directorate;
- Bolstering the powers of the Australian Federal Police and Australian Criminal Intelligence Commission to identify individuals and their networks engaging in serious criminal activity on the dark web, through the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021;*
- Progressing legislation to uplift the security and resilience of Australia's critical infrastructure, build our collective understanding of the threat environment, and ensure Government can assist industry in responding to cyber threats that are too sophisticated or disruptive to be handled alone;
- Developing the next National Plan to Combat Cybercrime, which will bring together the powers, capabilities, experience and intelligence of all jurisdictions to build a strong multi-faceted response to cybercrime harming Australia and Australians, consistent with the *National Strategy to Fight Transnational, Serious and Organised Crime*;
- Helping businesses by providing technical cyber security advice from the Australian Cyber Security Centre on how to prepare for, and respond to, ransomware attacks;
- Providing $6.1 million for support services through IDCARE to support Australians online, if they have been a victim of cybercrime (as part of the $1.67 billion);
- Helping small and medium business improve their cyber security through the free Cyber Security Assessment Tool;
- Improving the quality and quantity of skilled cyber security professionals through the Cyber Security National Workforce Growth Program, supporting businesses across the economy;
- Launching the 2021 International Cyber and Critical Technology Engagement Strategy with $20.5 million to strengthen cyber and critical technology resilience in Southeast Asia and $17 million to boost capability, including fighting cybercrime, in the Pacific; and
- Working collaboratively with international partners to address ransomware globally.

The Australian Government does not condone the payment of ransoms to cybercriminals. Australia is, and must continue to remain, a hard target for ransomware gangs. Payment of a ransom does not guarantee the victim access to its system or data and puts other Australians at greater risk.

Ransomware Action Plan

By complementing current initiatives, this Plan will ensure that Australia remains a hard target for cybercriminals. The Australian Government will:

- Launch additional operational activity to target criminals seeking to disrupt, and profit from, Australian business and individuals.
- Deliver additional legislative reforms to build Government's situational awareness of the ransomware threat while further criminalising ransomware (including by developing aggravated offences for attacks against Australia's critical infrastructure) and ensuring law enforcement can track, seize or freeze ransomware gangs' proceeds of crime.

The successful implementation of this Plan relies on close partnerships across industry and governments. The Australian Government will work closely with State and Territory governments and industry stakeholders to ensure that objectives of this Plan are achieved while complementing and not duplicating existing cyber security initiatives across the economy. We will leverage a range of existing engagement mechanisms to mobilise a national response to the threat of ransomware.

The Ransomware Action Plan is built on three objectives delivering initiatives in the immediate and mid-term.

Objectives

Prepare and Prevent	Respond and Recover	Disrupt and Deter
Building Australia's resilience to ransomware attacks.	Strengthening responses to ransomware attacks by ensuring support is available to victims.	Disrupting cybercriminals through deterrence and offensive action by strengthening Australia's criminal law regime and increasing the risk of ransomware gangs being caught.

Policy & Operational response

- Establishment of the multi-agency taskforce Operation Orcus as Australia's strongest response to the surging ransomware threat, led by the Australian Federal Police
- Awareness raising and clear advice for critical infrastructure, large businesses and small to medium enterprises on ransomware payments
- Joint operations with international counterparts to strengthen shared capabilities to detect, investigate, disrupt and prosecute malicious cyber actors when engaging in ransomware
- Actively calling out those who support, facilitate or provide safe havens to cybercriminals

Legislative reforms

- Introducing a specific mandatory ransomware incident reporting to the Australian Government
- Introducing a stand-alone offence for all forms of cyber extortion
- Introducing a stand-alone aggravated offence for cybercriminals seeking to target critical infrastructure (as proposed to be regulated by the Security Legislation Amendment (Critical Infrastructure) Bill 2020)
- Modernising legislation to ensure that cybercriminals are held to account for their actions, and law enforcement is able to track and seize or freeze their ill-gotten gains

Prepare and Prevent

Preparation and prevention are at the forefront of managing the risk of ransomware attacks.

There are a number of **current and immediate initiatives** which support ransomware preparation and prevention for all Australians, including:

- the Australian Cyber Security Centre's technical advice at cyber.gov.au, including the *Ransomware Prevention and Protection Guide,* and the *Emergency Response Guide*;
- the Australian Cyber Security Centre's '*act now, stay secure*' campaign, launched in December 2020, provides practical advice for Australians on how to protect themselves against a range of cyber threats, including ransomware;
- Initiatives funded under the Australian Signals Directorates' CESAR package, including partnership programs and alerts, as well as information sessions at Joint Cyber Security Centres;
- as a $4.9 million initiative under *Australia's Cyber Security Strategy 2020*, work is underway to commence a national cyber security public awareness campaign;
- the 2021 *International Cyber and Critical Technology Engagement Strategy* with $20.5 million to strengthen resilience in Southeast Asia and $17 million to boost capability, including fighting cybercrime, in the Pacific;
- uplifting the cyber security posture of Australia's critical infrastructure and systems of national significance through the Security Legislation Amendment (Critical Infrastructure) Bill 2020 and revitalised Trusted Information Sharing Network;
- practical advice for businesses, including through the release of the Cyber Security Industry Advisory Committee's public paper *Locked Out: Tackling Australia's ransomware threat*; and
- the Government is also seeking feedback on other regulatory reforms or voluntary incentives needed to promote the cyber security resilience of Australia's digital economy.

Future and ongoing work to support preparatory and prevention initiatives include:

- as part of *Australia's Cyber Security Strategy 2020*, the Australian Government is considering legislative changes, voluntary measures and incentives to strengthen cyber security across the digital economy;
- strengthening information sharing mechanisms;
- providing advice for critical infrastructure, large businesses and small to medium enterprises; and
- supporting initiatives to actively prevent known malicious cyber threats from reaching Australian consumers and businesses.

Respond and Recover

Strengthened response mechanisms for ransomware victims will help protect Australia and reduce the incentive to pay ransoms. Ransomware perpetrators should not be rewarded for their actions. Effective response initiatives must adopt a nationally consistent approach which provides incentives to victims to consider alternatives before paying ransoms. Paying ransoms is critical to the ransomware perpetrators' business model and will make Australia a more attractive target for criminals. Paying a ransom does not guarantee a successful outcome - encrypted systems may not be restored, sensitive data may be released or sold to other perpetrators and victims may be targeted multiple times.
The Australian Government has a number of **current and immediate initiatives** including:

- the Australian Cyber Security Centre's ReportCyber which allows Australian businesses or individuals to report a cyber incident, including a ransomware attack;
- the Notifiable Data Breaches scheme under the *Privacy Act 1988* requires Australian government agencies and certain Australian businesses to report ransomware attacks that involve a breach of personal information likely to result in serious harm;
- building Australia's collective understanding of the threat environment, and ensure Government can assist industry in responding to cyber threats that are too sophisticated or disruptive to be handled alone, through the Security Legislation Amendment (Critical Infrastructure) Bill 2020;
- providing $6.1 million for support services through IDCARE to support Australians if they have been a victim of cybercrime;
- clearly stating that the Australian Government does not condone the payment of a ransom to cybercriminals; and
- promoting information sharing and advice to assist industry, businesses and the community to make informed decisions before, during and after ransomware incidents.

Future and ongoing work to support response initiatives include:

- legislative reforms to ensure law enforcement can investigate and seize ransomware payments; and,
- legislative reforms to specifically mandate ransomware incident reporting to the Australian Government.

The Australian Government's policy is that it does not condone paying ransoms to cybercriminals. There is no guarantee that the payment will lead to your data being recovered, that the data won't be on-sold, or that you will not be attacked again.

Disrupt and Deter

Engaging in disruption and deterrence measures directly aimed at ransomware perpetrators is a key aspect of Australia's arsenal. This is achieved through cyber offensive capabilities and deterring cybercriminal strategies and business models. By taking an offensive approach, perpetrators are less likely to assess Australia as a vulnerable target.

Current and immediate initiatives include:

- establishing a new multi-agency law enforcement operation led by the Australian Federal Police (Operation Orcus) to crack down on the rising ransomware threat, both in Australia and overseas;
- strengthening Australia's capability to counter cybercrime through a $164.9 million investment, including $89.9 million to equip the Australian Federal Police with an additional 100 personnel to identify, investigate and target cybercriminals through *Australia's Cyber Security Strategy 2020*;
- establishing new powers through the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021*, to equip the Australian Federal Police and the Australian Criminal Intelligence Commission to identify individuals and their networks engaging in serious criminal activity on the dark web through network activity, data disruption and account takeover warranted powers;
- in 2016, establishing the Australian Cyber Security Centre as the standing taskforce that combines the expertise of foreign and domestic law enforcement and intelligence agencies to fight cybercrime, including countering ransomware;
- utilising the Australian Signals Directorate's offshore offensive cyber capabilities to disrupt foreign cybercriminals targeting Australian households and businesses;
- working with international partners to coordinate international disruption effort; and
- collaborating with states and territories to develop the next National Plan to Combat Cybercrime, which will bring together the powers, capabilities, experience and intelligence of all our jurisdictions to build a stronger operational response to cybercrime harming Australia and Australians.

Future and ongoing work to build disruption and deterrence initiatives include:

- legislative reforms to ensure that cybercriminals are held to account for their actions, and harsher penalties apply to those who engage in ransomware or target Australia's critical infrastructure;
- joint operations with international counterparts to strengthen shared capabilities to detect, investigate, disrupt and prosecute malicious cyber actors that engage in ransomware;
- actively calling out states who support or provide safe havens to cybercriminals; and
- tackling cryptocurrency transactions associated with the proceeds of ransomware crimes.

Future

The world has never been more interconnected and our reliance on the internet to fuel Australia's prosperity and maintain our way of life has never been greater.

Australia's response to the COVID-19 pandemic has shown the importance of secure online connectivity. It has also shown Australians' resilience and resolve to work towards a common goal. That same whole-of-nation partnership between government, businesses and the community must also be applied to ensuring Australia is cyber secure.

By complementing a range of existing initiatives, this Plan will ensure that cybercriminals and ransomware have no place in Australia.

We will:

- take action to become a hardened target for criminals seeking to disrupt and profit from Australian business and individuals;
- launch additional operational activity to target criminals attacking Australia through ransomware; and
- build better resilience by reviewing our regulations and strengthening our measures while further criminalising ransomware, including harsher penalties for those who attack Australia's critical infrastructure.

Together we will grow Australia's future as a modern and leading digital economy – safely, securely and with the highest levels of trust and confidence.

> ***Together we will grow Australia's future as a modern and leading digital economy – safely, securely and with the highest levels of trust and confidence.***