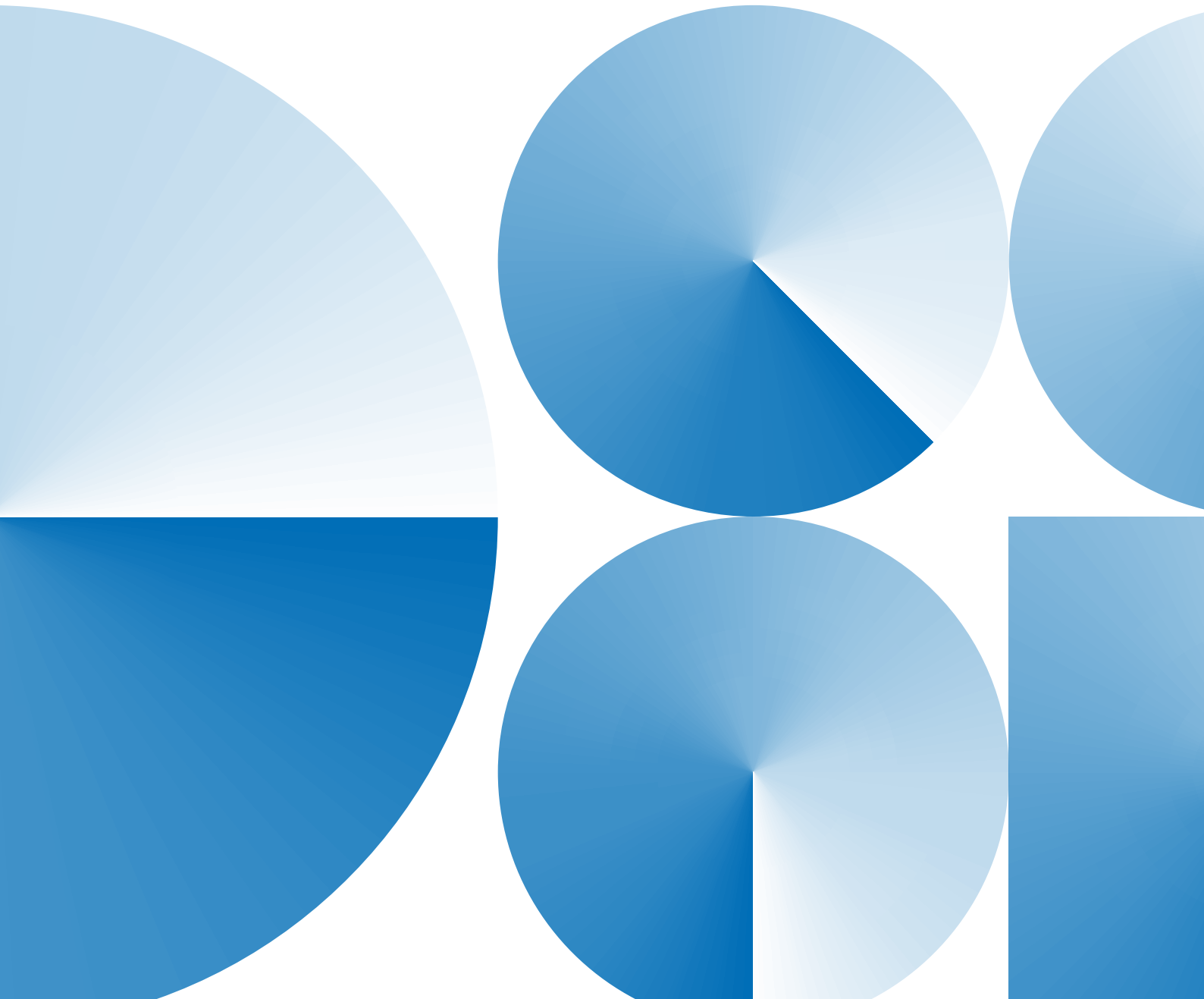
Australian Government
Australian Signals Directorate

ASD

The Commonwealth Cyber Security Posture in 2022

REPORT TO PARLIAMENT

December 2022



Use of the Coat of Arms

The Commonwealth Coat of Arms is used in accordance with the April 2014 Commonwealth Coat of Arms: Information and Guidelines, published by the Department of the Prime Minister and Cabinet and available online (http://www.itsanhonour.gov.au/coat-arms/index.cfm).

Website

www.cyber.gov.au

Contact us

Feedback about this report is welcome and should be directed to:

Phone

1300 CYBER1 (1300 292 371)

Email

asd.assist@defence.gov.au

Post

PO Box 5076, Kingston ACT 2604

Table of Contents

List of Figures

Executive summary

The Commonwealth Cyber Security Posture in 2022 (the report) informs Parliament on the implementation of cyber security measures across the Commonwealth government, for the period January 2021 to June 2022. As of June 2022, the Commonwealth comprised 97 non-corporate Commonwealth entities (NCCEs), 71 corporate Commonwealth entities (CCEs) and 17 Commonwealth companies (CCs). Throughout this report, the term 'entities' refers to all NCCEs, CCEs and CCs combined.

For the purposes of this report, an entity's cyber security posture comprises the following four dimensions:

i. Cyber security hardening: the entity's implementation of cyber security mitigations, primarily the Essential Eight mitigation strategies, to reduce the likelihood of an information communications technology (ICT) system being compromised.
ii. Incident preparedness and response: the entity's readiness to respond to cyber security incidents.
iii. Leadership and planning: the entity's leadership engagement with cyber security to support a strong cyber security culture.
iv. Cyber defence services: the entity's engagement with cyber defence services that detect and stop malicious cyber activity before it can impact a network.

The data included in this report is primarily derived from the *ASD Cyber Security Survey for Commonwealth Entities*. The Australian Signals Directorate (ASD) surveys entities annually regarding their cyber security practices. The survey addresses entities' implementation of the *Essential Eight Maturity Model*[1]; leadership and culture; incident management; and engagement with ASD services. NCCEs are required to respond to the survey under *Policy 5: Reporting on Security*[2] of the *Protective Security Policy Framework (PSPF)*[3]; all other entities are encouraged to respond. This year, 92% of entities participated in the survey. This data was supplemented by information collected by ASD in the performance of its duties.

At various points in this report, reference is also made to relevant findings from the *Protective Security Policy Framework (PSPF) Assessment Report 2020–21* (hereafter referred to as the PSPF Assessment Report)[4], published by the Attorney-General's Department (AGD). Each financial year, NCCEs must report on their security posture to AGD, with particular reference to implementation of government policies under the PSPF. The PSPF Assessment Report is an aggregated assessment of these findings. That report provides assurance to g overnment and the Australian public that entities are implementing security measures that proportionately address their unique security risk environments.

The findings presented here indicate that the cyber security posture across the Commonwealth is well-established in some areas but requires improvement in others. Specifically:

i. Essential Eight maturity levels improved, but remain low, across the Commonwealth.
    - The proportion of entities that have reached Overall Maturity Level 2 through implementation of Essential Eight controls alone increased from 4% in 2021 to 11% this year.
    - The proportion of entities that self-assessed as having reached Maturity Level 2 when compensating controls are taken into account increased from 14% in 2021 to 19% this year.

1. *Essential Eight Maturity Model*, ACSC website
2. *Policy 5: Reporting on security*, PSPF website
3. *Protective Security Policy Framework*, PSPF website
4. *Protective Security Policy Framework Assessment Report 2020–21*, PSPF website

ii. Most entities had prepared for a cyber security incident and were ready to respond as needed. However, the number of entities that had exercised their Incident Response Plan every two years, and the number of entities reporting incidents to the Australian Cyber Security Centre (ACSC), was relatively low.

- 79% of entities had an Incident Response Plan; however, only 49% of entities exercised their Incident Response Plan at least every two years.
- 80% of entities reported at least 80% of cyber security incidents to their senior management.
- 47% of entities reported 20% or fewer cyber security incidents to the ACSC.
- In 2021–22, entities reported 255 cyber security incidents to the ACSC, accounting for 23% of all cyber security incidents reported.

iii. There was a general improvement in cyber security leadership and planning across the Commonwealth. However, improvements could be made regarding entities' delivery of cyber security training to their workforces.

- 72% of entities had a cyber security strategy, up from 61% in 2021.
- 68% of entities provided cyber security training for their workforce at least annually.
- 34% of entities provided privileged user training at least annually.

iv. Engagement with ASD's cyber defence services is low to moderate.

- 2% of entities have joined the Cyber Threat Intelligence Sharing (CTIS) platform.
- 26% of entities were using the Australian Protective Domain Name System (AUPDNS).
- 38% of entities were protected by the Domain Takedown Service.

Against this backdrop, the ACSC will help entities improve their cyber security posture. The ACSC will seek to:

i. increase the number of entities engaging with the Cyber Maturity Measurement Program (CMMP) and ACSC Cyber Security Uplift Services for Government (ACSUSG)

ii. support entities to establish and exercise an Incident Response Plan

iii. investigate why some entities report a low percentage of incidents to the ACSC, and identify remediation measures

iv. encourage improved rates of annual cyber security workforce training across the Commonwealth

v. increase the number of entities utilising CTIS, AUPDNS and the Domain Takedown Service.

1. Introduction

Improving the cyber security of Australia's public, private and civil sectors is a priority of the Australian Government. As Australians increasingly rely on the internet and internet-connected devices, the scale of cyber risk continues to grow. Throughout the past year, Australia was the target of malicious cyber actors who, through persistent cyber operations, put Australia's security, stability and prosperity at risk.

The Australian Government plays an important role in monitoring, shaping and enabling cyber security across the economy. In particular:

i. ASD – through the ACSC – provides cyber security advice and assistance to Australian governments at the federal, state, territory and local levels, business and critical infrastructure, as well as communities and individuals.

ii. The Department of Home Affairs (Home Affairs) leads Australia's national cyber security policy and strategy, driving cyber security policy improvements across government and industry.

iii. AGD manages the PSPF, which sets out government protective security policy and supports entities to effectively implement that policy.

iv. The Digital Transformation Agency (DTA) drives digital transformation across government by providing strategic and policy leadership, and investment advice and oversight.

Within this context, entities – that is, the Australian Government's own departments and agencies – are responsible for maintaining the cyber security of their data and networks. Specifically, each entity is responsible for the security of its own ICT systems pursuant to the *Public Governance, Performance and Accountability Act 2013* (PGPA Act). Under the PSPF, an entity's accountable authority must approve an appropriate security plan to manage security risks.

This report provides an assessment of the cyber security posture of entities as at 30 June 2022, covering progress made by entities from 1 January 2021. It is the third report prepared in response to the Joint Committee of Public Accounts and Audit's *Report 467: Cybersecurity Compliance*[5], published in October 2017, which recommended that ASD and AGD report to Parliament annually on the cyber security posture of the Commonwealth. The annual reports are intended to support increased transparency in cyber security reporting.

1.1 Key findings of this report

The data included in this report is primarily derived from the annual *ASD Cyber Security Survey for Commonwealth Entities*. NCCEs are required to respond to the survey under *Policy 5: Reporting on security;* all other entities are encouraged to respond. This year, 92% of entities participated in the survey. This data was supplemented by information collected by ASD in the performance of its duties.

At various points in this report, reference is also made to relevant findings from the PSPF Assessment Report, published by AGD. Each financial year, NCCEs must report on their security posture to AGD, with particular reference to the implementation of government policies under the PSPF. The PSPF Assessment Report is an aggregated assessment of these findings. That report provides assurance to government and the Australian public that entities are implementing security measures that proportionately address their unique security risk environments.

Insight into the cyber security posture of individual entities may increase their risk of being targeted by adversaries. As such, this report does not identify entities by name. Instead, all data has been anonymised. Only aggregated results are provided.

5. *Report 467: Cybersecurity Compliance*, Parliament of Australia website

For the purposes of this report, an entity's cyber security posture comprises four dimensions:

i. Cyber security hardening: the implementation of cyber security mitigations – primarily the Essential Eight mitigation strategies – to reduce the likelihood of an entity's ICT systems being compromised.

ii. Incident preparedness and response: the entity's readiness to respond to cyber security incidents.

iii. Leadership and planning: the entity's leadership engagement with cyber security, to support a strong cyber security culture.

iv. ASD cyber defence services: the entity's engagement with cyber defence services that serve to detect and stop malicious cyber activity before it can impact a network.

The findings presented here indicate that the cyber security posture across the Commonwealth is well-established in some areas, but requiring improvement in others. Specifically:

i. Essential Eight maturity levels remained low, though improving, across the Commonwealth.

ii. Most entities had prepared for a cyber security incident and were ready to respond as needed. However, the number of entities that had exercised their Incident Response Plan every two years, and the number of entities reporting incidents to the ACSC, was relatively low.

iii. There was a general improvement in cyber security leadership and planning across the Commonwealth; most entities had a cyber security strategy. However, improvements could be made with regard to entities' delivery of cyber security training to their workforces.

iv. Engagement with ASD's cyber defence services is low to moderate.

The remainder of this report provides more detail on these findings and outlines next steps for improvement.

i. Section 2 outlines findings relating to the Commonwealth's implementation of technical controls to defend entities' ICT environments against cyber security threats.

ii. Section 3 outlines findings relating to entities' planning and preparedness to respond to adverse cyber security incidents.

iii. Section 4 outlines findings regarding the leadership and planning that underpins entities' cyber security culture.

iv. Section 5 outlines findings regarding entities' adoption of cyber defence services provided by ASD.

v. Finally, Section 6 summarises the key findings and offers next steps in the improvement of the Commonwealth cyber security posture.

2. Cyber security hardening

The implementation of cyber security controls helps entities defend their ICT environments against a range of threats, thereby avoiding costly remediation, downtime and lost productivity, and loss of public confidence. In relation to network hardening, the cyber security posture of entities was assessed using two data sets:

i. Responses to the *ASD Cyber Security Survey for Commonwealth Entities*, where entities report whether they have implemented controls recommended by the *Essential Eight Maturity Model*. Based on those responses, ASD calculates the entities' maturity level.

ii. Cyber Hygiene Improvement Programs (CHIPs) results. CHIPs is an open-source intelligence capability that uses objective and data-driven approaches to detect external indicators of network vulnerability.

2.1 Essential Eight Maturity Model

The ACSC's *Essential Eight Maturity Model* outlines a set of mitigation strategies to help organisations reduce their likelihood of experiencing a cyber security incident, and the impact of the incident if they do.

In 2020, ASD conducted a review of the Essential Eight to ensure that it remained contemporary and contestable. This review was based on the Essential Eight assessments carried out across the Commonwealth, engagement with government entities to understand their experiences implementing the Essential Eight, and awareness of the constantly evolving cyber threat environment. In July 2021, the updated *Essential Eight Maturity Model* was published on cyber.gov.au.

2.1.1 Implementation of the Essential Eight Maturity Model

The *Essential Eight Maturity Model* comprises four maturity levels (Maturity Levels 0 to 3). The higher levels of maturity protect entities against moderate-to-high degrees of sophistication in adversary tradecraft and targeting. As of July 2022, it is a core requirement of the PSPF that entities implement the Essential Eight strategies to at least Maturity Level 2. A network's Overall Maturity Level is equal to its least mature strategy.

The *Essential Eight Maturity Model* comprises the following eight strategies:

1. **Application control:** ensures only corporately approved software applications can be executed on a computer, protecting against the execution of malicious applications.
2. **Patch applications:** applying vendor patches or other vendor mitigations prevents known vulnerabilities in applications from being exploited.
3. **Configure Microsoft Office macro settings:** limits macro programs embedded in Microsoft Office files from executing, thereby preventing potential malicious activity.
4. **User application hardening:** limits the use of potentially exploitable user application functionality to only what is required, and removes particularly vulnerable software altogether.
5. **Restrict administrative privileges:** limits the unnecessary provision of administrative privileges, reducing the potential for these to be exploited by adversaries to gain full access to computers and data.
6. **Patch operating systems:** applying vendor patches or other vendor mitigations prevents known vulnerabilities in operating systems from being exploited.
7. **Multi-factor authentication:** requires users to present multiple authentication credentials to log in, rather than just using a passphrase, thereby preventing adversaries logging in as a user if they know the user's passphrase.
8. **Regular backups:** making a copy of data, software and configuration settings, storing it securely and periodically testing the ability to restore it, enables data and computers to be restored after an incident such as ransomware or computer hardware failure.

The *Essential Eight Maturity Model* recommends that organisations implement the Essential Eight using a risk-based approach. Where strategies cannot be implemented, these exceptions should be minimised and compensating controls used to manage the resulting risk. If the gap is effectively mitigated, the entity may self-assess that they have achieved maturity against that strategy.

2.1.2 Level of Essential Eight implementation by entities

The vast majority of entities have not implemented all the Essential Eight mitigation strategies to Maturity Level 2. Specifically:

- **i.** Only 11% of entities had reached Overall Maturity Level 2, relying on the implementation of Essential Eight controls alone; an increase from 4% in 2021.
- **ii.** 19% of entities self-assessed that they had reached Maturity Level 2 when compensating controls to mitigate gaps in the Essential Eight implementation were taken into account; an increase from 14% in 2021.
- **iii.** Between 2021 and 2022, the greatest improvements to the number of entities implementing an Essential Eight strategy to Maturity Level 2 were observed in Patch applications (26% improvement) and Patch operating systems (24% improvement) (Figure 1).
- **iv.** Regular backups, Application control and Patch operating systems were implemented to Maturity Level 2 by the highest proportion of entities, following the application of compensating controls (Figure 2).
- **v.** User application hardening and Restrict administrative privileges were implemented to Maturity Level 2 by the lowest proportion of entities, following the application of compensating controls (Figure 2).

2.1.3 Protective Security Policy Framework Report 2020–21

The PSPF Assessment Report includes reporting against *Policy 10: Safeguarding data from cyber threats*[6]. In 2020–21, this policy mandated the implementation of four of ASD's Essential Eight mitigation strategies: Application control, Patch applications, Restrict administrative privileges, and Patch operating systems.

The PSPF Assessment Report found that 28% of entities had implemented these strategies to a 'Managing' or 'Embedded'[7] level.

From July 2022, the PSPF requires entities to implement Maturity Level 2 for each of the Essential Eight strategies.

6. *Policy 10: Safeguarding data from cyber threats*, PSPF website.
7. Under the PSPF maturity model, a 'Managing' maturity level means there has been '[c]omplete and effective implementation' of a given aspect of the PSPF. An 'Embedded' maturity level means there has been '[c]omprehensive and effective implementation' of that aspect of the PSPF.

FIGURE 1: Percentage of entities with Essential Eight Maturity Level 2 or higher (Essential Eight strategies only)

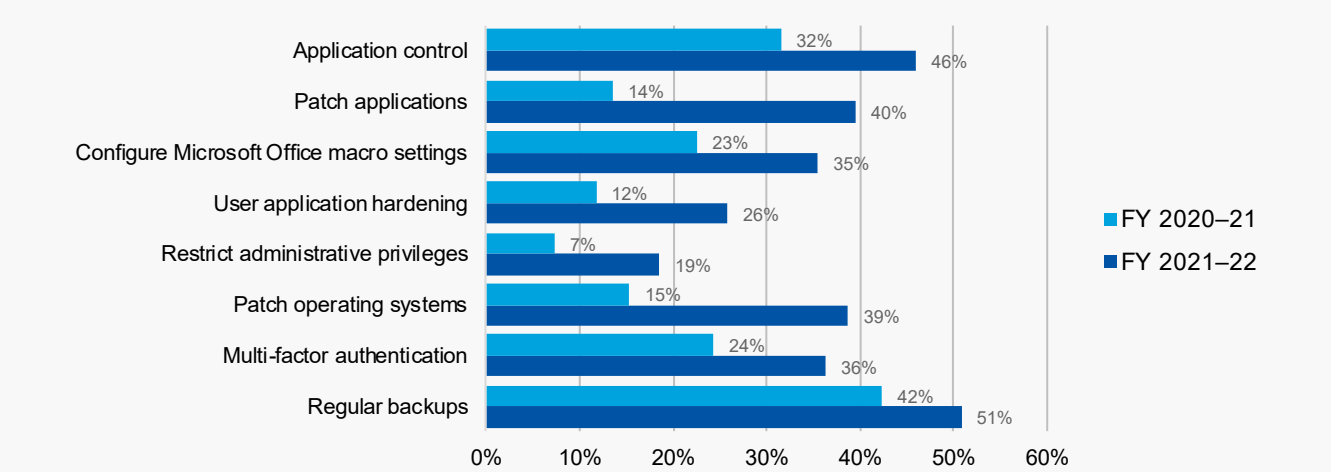
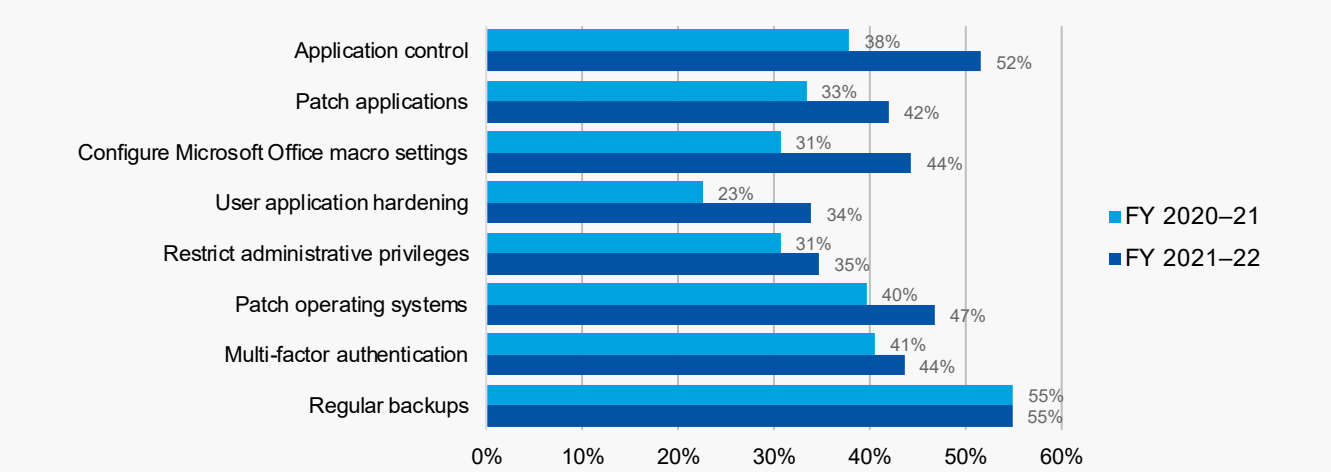


FIGURE 2: Percentage of entities with Essential Eight Maturity Level 2 or higher (Essential Eight plus compensating controls)



2.2 Cyber Hygiene Improvement Programs scanning (CHIPs)

CHIPs scans provide information to entities on a range of cyber hygiene indicators, identifying areas of cyber security concern. Over the reporting period, the proportion of domains protected by key security measures increased, while the number of domains hosting dormant websites decreased. Specifically, between February 2021 and May 2022:

- **i.** use of recommended email security[8] rose from 8.0% to 61.3%
- **ii.** use of recommended email encryption[9] rose from 17.9% to 41.6%
- **iii.** use of recommended web server encryption[10] rose from 15.2% to 28.6%
- **iv.** the existence of dormant websites (which might be used to host or launch malicious activity) decreased from 15.0% to 8.8%.

These results are further described in Figure 3 to Figure 6.

CHIPs reporting indicates that entities are improving their overall implementation of the security protocols above. However, the proportion of Commonwealth domains in which these cyber hygiene measures have not been effectively implemented remains high.

Case Study 1: Support to the 2021 Census

In August 2021, the Australian Bureau of Statistics (ABS) ran the eighteenth Census of Population and Housing (Census) in Australia. From planning through to delivery, ASD provided ABS with cyber security advice, assistance and technical uplift to help ensure the cyber security of the Census and its data.

Prior to the Census, ASD provided ABS with cyber security advice for its procurement process, a cyber security maturity assessment across ABS networks, a review of the platform hosting the Census, and threat intelligence briefings. ASD employed its cyber defence service capabilities to assess and pre-empt malicious cyber activity against the Census.

Throughout the Census, ASD was in constant communication with ABS and conducted passive monitoring of the ABS systems and incident response support to help detect and respond to threats. On Census night, ASD provided on-site operational support to bolster any critical incident response.

ASD found no indication of malicious activity through its assessments, and critical cyber security recommendations were resolved by ABS prior to the Census. The 2021 Census was completed successfully without cyber security incident.

8. Recommended email security: Sender Policy Framework (SPF) and Domain-based Message Authentication Reporting and Conformance (DMARC).
9. Recommended email encryption: Transport Layer Security (TLS) and Mail Transfer Agency Strict Transport Security (MTA-STS).
10. Recommended web server encryption: Hypertext Transfer Protocol Security (HTTPS) and HTTP Strict Transport Security (HSTS).

FIGURE 3: Implementation of email security measures across entities' domains

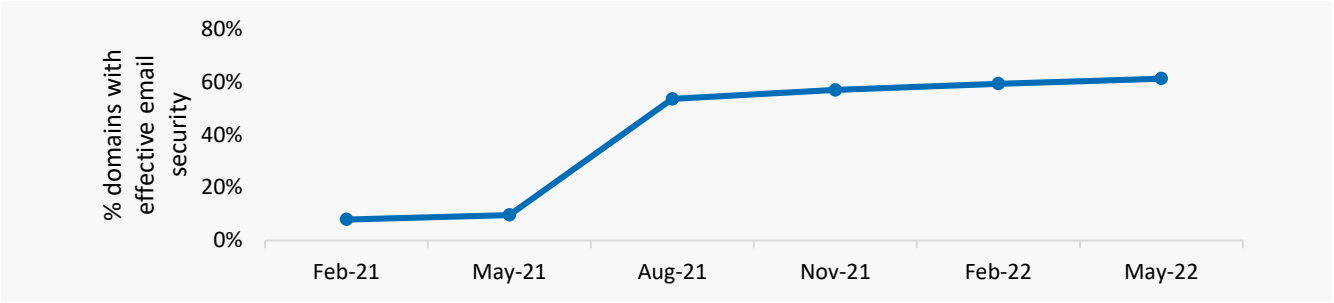


FIGURE 4: Implementation of email encryption by device across entities' domains

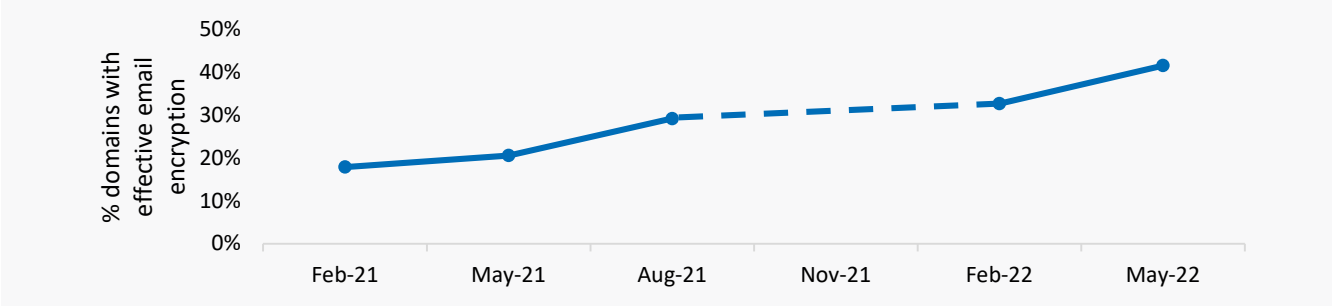


FIGURE 5: Implementation of website encryption across entities' domains

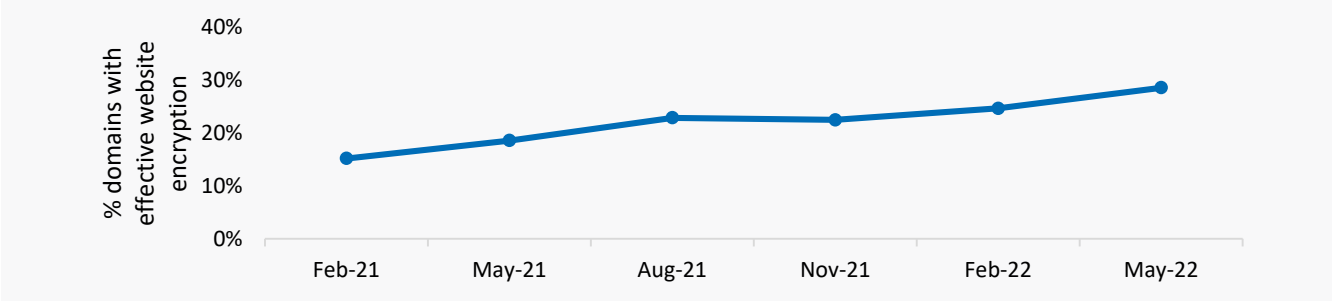
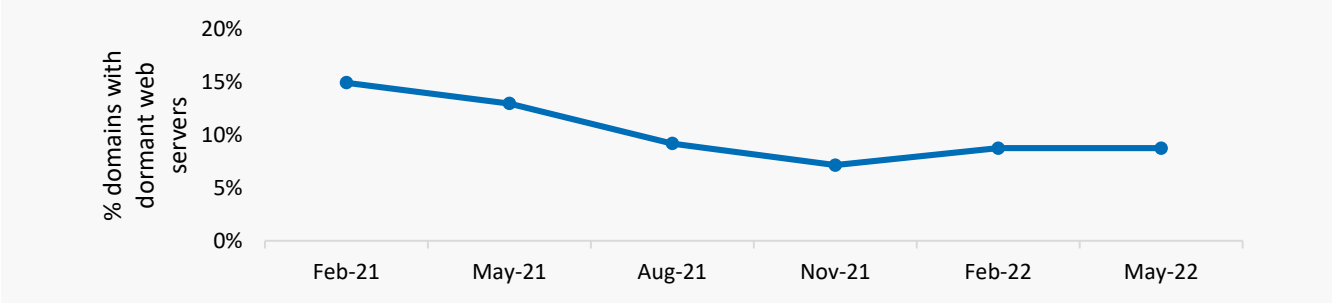


FIGURE 6: Dormant websites across entities' domains



3. Incident preparedness and response

A cyber security event occurs when a system, service or network flags a possible breach of security policy, failure of safeguards or a previously unknown situation that may be relevant to security. A cyber security incident is an unwanted or unexpected cyber security event, or a series of such events, that have a significant probability of compromising business operations.

Cyber security incidents may result in the denial of access to, the theft of, or the destruction of systems and data. If not effectively managed, a cyber security incident may undermine public confidence in an organisation, and the incident's remediation may consume significant resources.

While it is important to defend against cyber security incidents, it is impossible to avoid them entirely. Entities should plan for, and prepare to respond to, cyber security incidents. This includes identifying the data and systems essential to their business, accounting for cyber security incidents in business continuity planning, and developing and exercising an incident response plan.

Reporting cyber security incidents is also essential to ensure that they are dealt with appropriately and that any impact is considered fully. According to *Policy 5: Reporting on security*, entities are required to report 'significant or reportable' cyber security incidents to the ACSC.

Entities are a common target for malicious cyber activity. In 2021–22, entities reported 255 cyber security incidents to the ACSC, accounting for 23% of all cyber security incidents reported.

3.1 Levels of incident preparedness and reporting

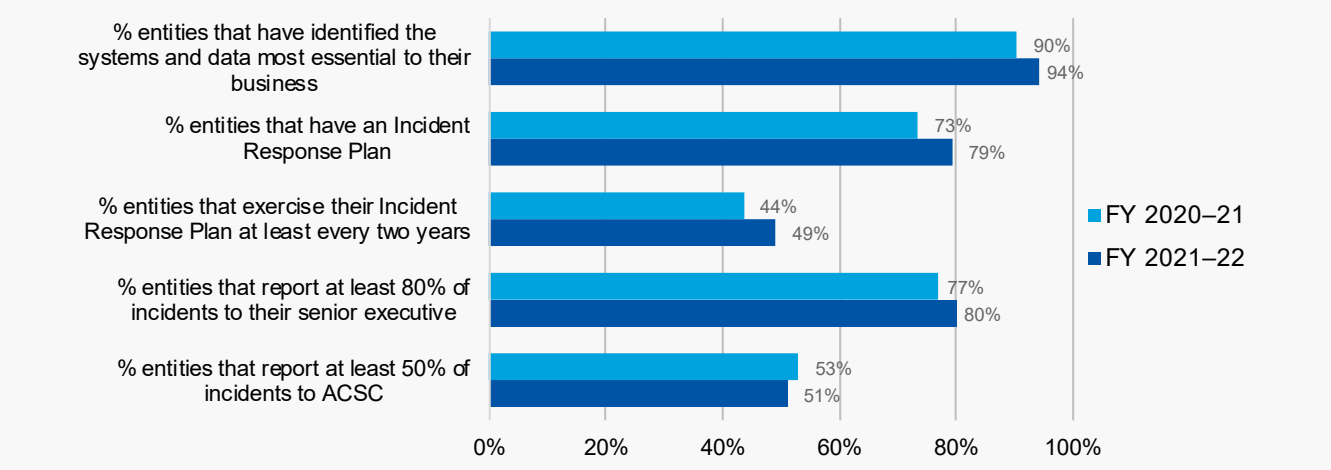
In relation to incident preparedness and response, the cyber security posture of entities is assessed using responses from the *ASD Cyber Security Survey for Commonwealth Entities*. Specifically, entities respond to a series of questions designed to assess their level of preparedness to respond to a cyber security incident, and their incident reporting behaviour.

Findings indicate that the majority of entities had planned for a cyber security incident, and were ready to respond, if needed. However, a much smaller proportion of entities had exercised their Incident Response plan. Specifically, as shown in Figure 7:

- **i.** 94% of entities had identified the systems and data most essential to their business; an increase from 90% in 2021.
- **ii.** 79% of entities had an Incident Response Plan; an increase from 73% in 2021.
- **iii.** 49% of entities exercised their Incident Response Plan at least every two years; an increase from 44% in 2021.

Notably, there was little change in these results between 2021 and 2022.

FIGURE 7: Indicators of entities' incident preparedness and response



While most entities report a high rate of cyber security incidents to their senior management, this is not the case with regard to reporting incidents to the ACSC. Rather, a large cohort of entities report all cyber security incidents to the ACSC, while a distinct cohort report relatively few cyber security incidents to the ACSC. As shown in Figure 7:

i. 80% of entities reported at least 80% of the incidents observed on their network to their senior management; an increase from 77% in 2021.

ii. 51% of entities reported at least 50% of incidents observed on their network to the ACSC, a minor decrease from 53% in 2021:

- 41% reported 100% of incidents observed on their network to the ACSC, increasing from 39% of entities in 2021.
- 47% reported 20% or fewer incidents observed on their network to the ACSC, increasing from 45% in 2021.
- 12% reported between 30% and 90% of incidents observed on their network to the ACSC, down from 16% in 2021.

Under *Policy 5: Reporting on Security*, entities are required to report 'significant or reportable' cyber security incidents to the ACSC. The low rate of incident reporting may have a variety of causes. Specifically:

i. A proportion of entities may be experiencing a high number of low-impact incidents that do not meet the reporting threshold.

ii. A proportion of entities may be experiencing reportable incidents, but do not recognise them as reportable.

Case Study 2: Log4j vulnerability response

The Log4j vulnerabilities were the most prevalent critical vulnerabilities in the 2021–22 financial year. On 10 December 2021, ASD issued a public alert, and commenced awareness and response initiatives to mitigate the potential compromise. Due to its widespread use in popular software and hardware platforms, over 100,000 products may contain Log4j.

Between December 2021 and January 2022, ASD provided technical support to impacted organisations, releasing 2 Alerts and 2 Advisories flagging the active exploitation. ASD also provided technical advice and guidance for mitigation and detection, hosted 7 information sharing events through the ACSC Partnership Program, and amplified advice on social media, which had a potential reach of over 1 million people. On 22 December 2021, ASD also released a joint public technical advisory on mitigations for Log4j-related vulnerabilities with the US, UK, Canada and New Zealand.

ASD is aware of malicious actors conducting a large number of reconnaissance scans for Log4j vulnerabilities. Some Australian networks were compromised through Log4j vulnerabilities, and ASD responded to over 50 cyber security incidents. ASD has identified Log4j exploits being used months after the initial disclosure. Log4j is likely to be a means of access for malicious actors for years to come.

Case Study 3: AquaEx

AquaEx, the national cyber security exercise series coordinated by ASD in partnership with Australian critical infrastructure owners and operators, was held in August 2021. The exercise brought together Australia's urban water and wastewater sector and government agencies, with the aim of strengthening industry and government coordinated response to cyber incidents affecting the sector.

The exercise was an opportunity for participants to reflect on existing communication and cooperation arrangements to respond to a cyber incident affecting industry, and how these arrangements can be improved. It enabled industry and government to clarify their roles and responsibilities, including reporting responsibilities for organisations affected by a cyber incident.

AquaEx involved over 14 months of planning, 50 one-on-one planning conferences, 16 exercise management workshops, 4 information sessions, and the development of a Cyber Incident Response Plan template to assist organisations in developing and updating their cyber incident response plans in preparation for the exercise.

Despite the challenges presented by COVID-19 lockdowns, the exercise had a record number of participants. In total, more than 750 participants, from 48 organisations (including 4 entities), took part in the activity, strengthening relationships and enhancing cyber awareness.

4. Leadership and planning

Strong leadership is essential in setting and maintaining a strong cyber security culture, and ensuring cyber security remains part of an organisation's planning and everyday business. In particular, the Chief Information Security Officer (CISO) plays a key role in setting the strategy and direction of an entity's cyber security program. CISOs are typically responsible for providing strategic guidance to their entity's cyber security program and ensuring compliance with cyber security policy, standards, regulations and legislation.

The broader workforce also plays a key part in maintaining cyber security, and entities should provide ongoing cyber security awareness training to all personnel to help them to understand their security responsibilities.

4.1 Levels of leadership and planning

In relation to leadership and planning, the cyber security posture of entities was assessed through a series of questions designed to provide indications of their entity's cyber security leadership, planning and overall culture.

Responses showed improvement on most indicators of leadership and planning (Figure 8). Specifically, as of June 2022:

i. 72% of entities had a cyber security strategy, up from 61% in 2021.

ii. 82% of entities addressed cyber security incidents in business continuity planning, up from 75% in 2021.

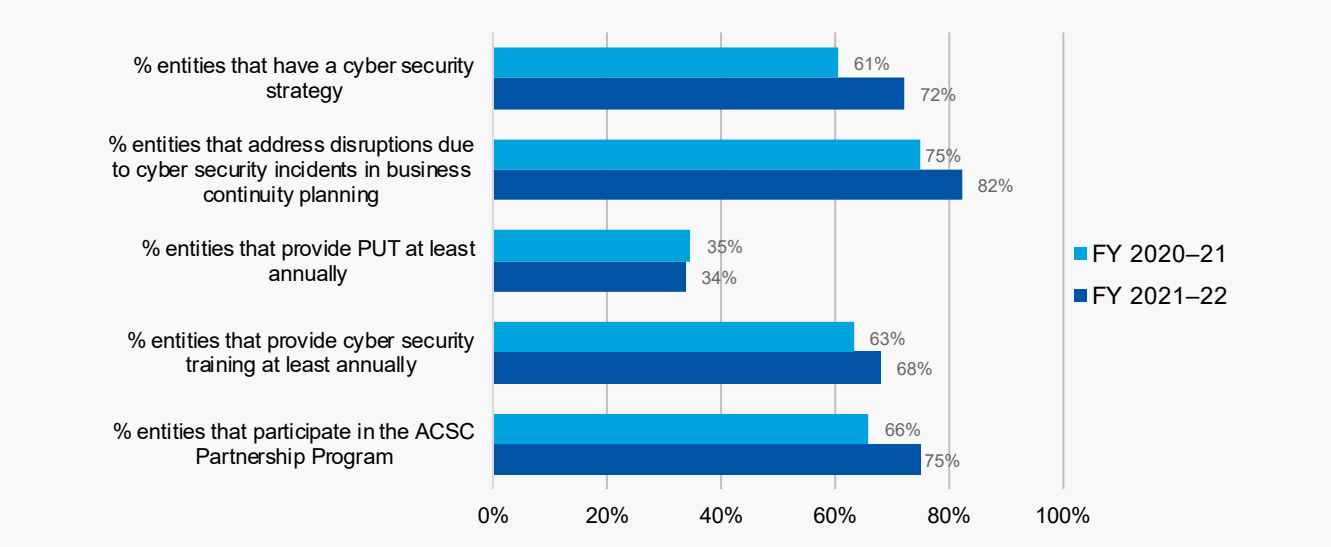
iii. 68% of entities provided cyber security training for their workforce at least annually, increasing from 63% in 2021.

iv. 75% of entities participated in the ACSC Partnership Program, increasing from 66% in 2021.

Ideally, all entities should engage in these activities. However, the increasingly high uptake across entities signals a general improvement in posture.

A notable exception is cyber security training. Responses indicate that 68% of entities provide cyber security training to their workforce at least annually, while 34% of entities provided privileged user training (PUT) to ICT users with elevated privileges at least annually.

FIGURE 8: Indicators of entities' leadership and planning



Case Study 4: Ransomware – Exercise Blue Dawn

Ransomware is one of the most disruptive threats to Australian organisations. In April 2022, ASD coordinated Exercise Blue Dawn, a simulated ransomware cyber security incident, for its Network Partners within the ACSC Partnership Program. The exercise supported participants from a range of sectors to clearly identify their strengths and weaknesses, and improved their holistic organisational responses to ransomware.

The 62 participating entities stated that they learned from each other's expertise and experiences with ransomware, incident response and planning. Conducting cyber security exercises such as this are an integral part of cyber security preparedness, where relevant personnel or organisations come together in a simulated environment to discuss, review and develop response plans, policies, and capabilities.

As a result of the exercise, participants indicated that they would review and further develop their organisations' incident response and preparedness plans. In addition, 98% agreed that Blue Dawn enhanced their ability to perform their roles under similar circumstances and that their participation was appropriate and beneficial to their roles. The ACSC continues to develop close collaboration opportunities for ACSC Network Partners to build cyber resilience and maturity for all Australian organisations.

Case Study 5: Australian Protective Domain Name System (AUPDNS)

AUPDNS enhances the security of government networks by blocking connections to malicious websites that may contain ransomware, malware and other cyber threats. ASD and its industry partner make this service available to all federal, state and territory governments. AUPDNS has proven to be invaluable for threat detection and intelligence gathering, as well as for disrupting or deterring cyberattacks at the reconnaissance phase.

Since the AUPDNS pilot began in March 2020, ASD has analysed abnormal Domain Name Service (DNS) traffic flows to detect possible malicious activity and, through this, either mitigate or reduce the harm of an intrusion for entity customers. AUPDNS has become the largest contributor of indicators of compromise to ASD's CTIS platform, providing over 80% of CTIS inputs.

During the reporting period, AUPDNS processed more than 30 billion queries and blocked more than 20 million connections to known malicious domains. By the end of the 2021–22 financial year, 49 entities were using the service. As more entities connect to AUPDNS, ASD achieves greater cyber threat visibility and defence.

5. Cyber defence services

The cyber defence services offered to entities by ASD are designed to detect and stop malicious cyber activity before it can impact organisations or the community. Cyber defence services are intended to tackle the high-volume attacks that affect many targets, from government entities to individual internet users, rather than highly sophisticated and targeted attacks. As such, these services are generally scalable and designed to block malicious cyber activity while in train. It is recommended that all entities take advantage of cyber defence services, either by accessing those provided by ASD or engaging a commercial service.

5.1 ASD services available to entities

ASD provides cyber defence services to entities to mitigate low-sophistication attacks before they impact the network, including:

i. **Cyber Threat Intelligence Sharing (CTIS)**

   In November 2021, ASD began operating the new CTIS platform. CTIS allows participating entities to share observable indicators of compromise (IOCs) at machine speed. Participating organisations can then use these IOCs to identify activity on their own networks. The CTIS platform also allows participating organisations to bi-directionally share IOCs observed on their own networks with other CTIS partners. Since its launch, 28,000 IOCs have been shared on CTIS.

ii. **Australian Protective Domain Name System (AUPDNS)**

   The AUPDNS uses threat intelligence to build a block list of known and assessed malicious web domains. These domains are often used to distribute malware, as part of malicious command-and-control channels, or as part of a data-exfiltration channel. AUPDNS prevents devices on subscribed networks from accessing the malicious domains on the block list, thereby interrupting potential malicious activity. Between 1 January 2021 and 30 June 2022, more than 20 million malicious domain requests were blocked by AUPDNS.

iii. **Domain Takedown Service**

   The Domain Takedown Service prevents malicious resources from being hosted on unsuspecting entities' web domains. The service detects potentially malicious activity that is using subscribed entities' web domains, verifies that this activity is malicious, and issues a takedown notification request to the Domain Host (i.e. the internet service that manages that domain). The majority of takedown notifications are automatically initiated within one minute of identification. Within the reporting period, 70,000 domain takedown notifications were sent to entities.

5.2 Uptake of ASD's cyber defence services

The uptake of ASD's cyber defence services was assessed using information collected by ASD as part of their normal operations. According to ASD records, as of 30 June 2022:

i. 2% of entities had joined the CTIS platform

ii. 26% of entities were using AUPDNS

iii. 38% of entities were protected by the Domain Takedown Service.

6. Conclusion and next steps

Cyber security must be a priority for all entities. The findings presented in this report indicate that the cyber security posture across the Commonwealth is well-established in some areas, but requiring improvement in others. In particular:

i. Most entities do not meet the minimum requirements for cyber security, as described in the *Essential Eight Maturity Model*. This conclusion is supported by the PSPF Assessment Report.

ii. Most entities had prepared for a cyber security incident, and were ready to respond as needed. However, the number of entities that had exercised their Incident Response Plan every two years, and the number of entities reporting incidents to the ACSC, was relatively low.

iii. There was a general improvement in cyber security leadership and planning across the Commonwealth. However, further improvements could be made with regard to entities' delivery of cyber security training to their workforces.

iv. Engagement with ASD's cyber defence services is low to moderate across the Commonwealth.

6.1 Next steps

Against this backdrop, entities should work to:

i. prioritise, and appropriately resource, improvements to their cyber security posture in line with the Essential Eight

ii. establish and exercise an effective cyber security Incident Response Plan

iii. review their cyber security incident reporting practices

iv. provide annual cyber security training and privileged user training across their workforce

v. seek to engage with ASD's cyber defence services.

The ACSC will help entities to improve their cyber security posture. The ACSC will:

i. increase the number of entities engaging with the Cyber Maturity Measurement Program (CMMP) and ACSC Cyber Security Uplift Services for Government (ACSUSG)

ii. support entities to establish and exercise an Incident Response Plan

iii. investigate why some entities report a low percentage of incidents to the ACSC, and identify remediation measures

iv. encourage improved rates of annual cyber security workforce training across the Commonwealth

v. increase the number of entities utilising CTIS, AUPDNS and the Domain Takedown Service.

6.2 Final comments

The importance of effective cyber security will continue to grow as the Commonwealth government increasingly relies on the internet and internet-connected devices. Entities continue to improve their cyber security posture. However, considerable improvement is still required to meet the rapidly evolving cyber threat environment.

6.3 Report to Parliament 2023

The Commonwealth Cyber Security Posture in 2023 Report to Parliament will be delivered in November 2023. This report will focus on the 2022–23 financial year.

ANNEX A: ASD Services for Commonwealth entities

Cyber security hardening

From 1 January 2021 to 30 June 2022...

1
major update to the *Essential Eight Maturity Model* was published in July 2021

678
ISM updates were published

11
entities engaged in CMMP

22
entities engaged in ACSUSG

212
IRAP-accredited assessors providing IRAP services

Quarterly
CHIPs scans were performed across government networks

62
HOT CHIPs scans were performed across government networks

Technical publications

ASD publishes the *Information Security Manual* (ISM), the *Essential Eight Maturity Model*, and the *Strategies to Mitigate Cyber Security Incidents,* all of which outline the technical strategies and controls designed to defend against cyber threats. ASD also publishes additional guidance on topics of particular relevance, such as cloud and gateway services.

Cyber Maturity Measurement Program (CMMP)

ASD's CMMP works with entities to assess their networks' implementation of the Essential Eight mitigation strategies and their broader cyber security posture. Entities are provided with a snapshot of their networks' cyber security posture and tailored advice and recommendations to improve.

ACSC Cyber Security Uplift Services for Government (ACSUSG)

ASD's ACSUSG service provides entities with skilled ICT professionals to implement security controls and provide further recommendations aligned with the ACSC's findings and advice provided through complementary offerings.

Information Security Registered Assessors Program (IRAP)

Through the IRAP, ASD endorses suitably qualified professionals to provide cyber security services to support broader industry and Australian Government. IRAP assessors can provide security assessments of ICT systems, cloud services and gateways.

Active Vulnerability Assessments (AVA)

AVA is ASD's 'red team' capability, designed to assess the network and system security of Australia's most critical, nationally significant and sophisticated infrastructure.

Cyber Hygiene Improvement Programs (CHIPs)

CHIPs uses open source techniques to measure the cyber posture and hygiene of government internet-facing systems and assets. It uses objective and data-driven approaches to detect external indicators that a network may be vulnerable to exploitation. CHIPs provides quarterly reports to Commonwealth, state, territory and local government entities, detailing vulnerability posture and findings for each entity.

High-Priority Operational Tasking Cyber Hygiene Improvement Programs (HOT CHIPs)

ASD's HOT CHIPs scans identify network and system vulnerabilities relating to high-priority threats. These scans build ACSC visibility of the government attack surface, and help network owners to build cyber hygiene quickly by providing timely and actionable threat intelligence.

Host Based Sensor Program (HBS)

ASD's HBS program provides visibility of the cyber security posture of Australian Government ICT systems by collecting telemetry data from government devices. This enables ASD to help entities identify weaknesses and detect intrusions on their ICT infrastructure, and mitigate the consequences of compromise.

Incident preparedness and response

From 1 January 2021 to 30 June 2022...

67
calls, on average, were received by the Cyber Security Hotline each day

55
entities engaged in a National Exercise Program exercise

3
Hunt activities were conducted for entities

30
exercises were run by the National Exercise Program

20
workshops were run by the National Exercise Program

3548
downloads of the Cyber Incident Response Plan were undertaken

Alerts and Advisories

ASD publishes alerts and advisories to cyber.gov.au to inform Australians on cyber security threats. Individuals may subscribe to the ACSC Alert Service to have such alerts forwarded to them automatically.

Cyber Security Hotline

The Australian Cyber Security Hotline '1300 CYBER1' (1300 292 371) provides advice and assistance to Australian individuals and organisations impacted by cyber security incidents. The Hotline is available 24 hours a day, seven days a week.

Incident Response

ASD provides incident response services to all entities that have been compromised by malicious cyber actors. ASD prioritises deployment of specialised digital forensics and incident response services in response to incidents causing significant impact to Australia and/or incidents involving high harm actors.

Hunt

ASD proactively conducts cyber threat hunt operations on important Australian networks to detect intrusions by sophisticated cyber actors. This service is offered to entities, including in support of events of national significance. In such cases, ASD is invited by the entity to conduct a hunt, and works in partnership with the entity for the duration of the hunt activity.

National Exercise Program (NEP)

The National Exercise Program (NEP) runs scalable and agile exercises to help participants validate and improve their cyber security arrangements. The NEP also runs cyber security training workshops for industry and government. ASD periodically runs large-scale exercises, such as AquaEx, described in Case Study 3.

Cyber Incident Response Plan and Readiness Checklist

In January 2022, the ACSC published a *Cyber Incident Response Plan Template* and *Cyber Incident Response Readiness Checklist* on cyber.gov.au. These documents are designed to help entities develop a cyber incident response plan to support an effective incident response.

Leadership and planning

From 1 January 2021 to 30 June 2022...

140
entities were invited to each CIO/CISO forum

110
entities were invited to each ITSA forum

39
ACSC newsletters were published to the Partnership Portal

119
entities were members of the ACSC Partnership Program

28%
of entities enrolled participants in PUT

Chief Information Officer (CIO)/CISO, Information Technology Security Advisor (ITSA) forums and newsletter

ASD runs a number of forums annually for Commonwealth government CIOs and CISOs, as well as additional forums for ITSAs. A newsletter is also published for participants.

The forums and newsletters bring together senior cyber security practitioners to discuss strategic cyber security matters, as well as technical topics and tools.

During the reporting period, ASD provided updates on the Hardening Government IT Initiative (HGIT), the Critical Infrastructure and Systems of National Significance (CISoNS) reforms, *Essential Eight Maturity Model* updates, and ASD incident response activities.

Lessons learned from the 2021 Tokyo Olympics and the 2021 Census were also provided by participating entities.

Partnership Program

The ACSC Partnership Program enables a wide range of organisations to engage with the ACSC. Through the Partnership Program, ACSC provides technical advisories, sector-based threat intelligence, news and advice to enhance situational awareness, collaboration opportunities, and resilience-building activities.

Privileged User Training (PUT)

ASD provides in-person and online Privileged User Training (PUT) for ICT users who hold system privileges beyond that of a normal user. Privileged users are technical staff with duties and system access that enable them to adjust and maintain the configurations of ICT systems.

The course provides an overview of best-practice cyber security, including mitigating cyber security incidents in privileged users' day-to-day work.

ASD's PUT is intended for entities that don't have the capacity or requirement to run in-house training for their privileged users. Entities may provide their own alternative.

Cyber defence services

From 1 January 2021 to 30 June 2022...

28,000
IOCs were shared via the CTIS platform.

20 million
malicious domain requests were blocked by AUPDNS

70,000
domain takedown notifications were sent to entities

Cyber Threat Intelligence Sharing (CTIS)

In November 2021, ASD began operating the new CTIS platform. CTIS allows participating entities to share observable indicators of compromise (IOCs) at machine speed. Participating organisations can then use these IOCs to identify activity on their own networks. The CTIS platform also allows participating organisations to bi-directionally share IOCs observed on their own networks with other CTIS partners.

Australian Protective Domain Name System (AUPDNS)

The AUPDNS uses threat intelligence to build a block list of known and assessed malicious web domains. These domains are often used to distribute malware, as part of malicious command-and-control channels, or as part of a data-exfiltration channel. AUPDNS prevents devices on subscribed networks from accessing the malicious domains on the block list, thereby interrupting potential malicious activity, see Case Study 5.

Domain Takedown Service

The Domain Takedown Service prevents malicious resources from being hosted on unsuspecting entities' web domains. The service detects potentially malicious activity that is using subscribed entities' web domains, verifies that this activity is malicious, and issues a takedown notification request to the Domain Host (i.e. the internet service that manages that domain). The majority of takedown notifications are automatically initiated within one minute of identification.

Intentionally blank

Intentionally blank