Australian Government
Australian Signals Directorate

ASD

The Commonwealth Cyber Security Posture in 2024

REPORT TO PARLIAMENT

NOVEMBER 2024

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the following website: https://pmc.gov.au/cca

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

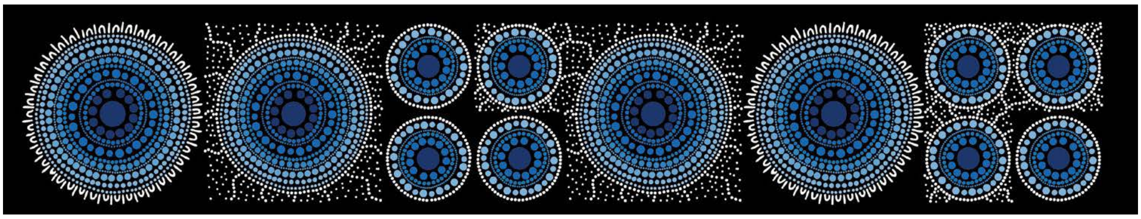
Post

PO Box 5076, Kingston ACT 2604

Acknowledgement of Country

We acknowledge the Traditional Owners and Custodians of Country throughout Australia and their continuing connections to land, sea and communities.

We pay our respects to them, their cultures and their Elders; past, present and emerging. We also recognise Australia's First Peoples' enduring contribution to Australia's national security.



Contents

List of Figures

Executive summary

The Commonwealth Cyber Security Posture in 2024 (hereafter the 'report') informs the Australian Parliament on cyber security measures implemented across the Australian Government for the 2023–24 financial year. According to the *Public Governance, Performance and Accountability Act 2013* Flipchart of Commonwealth entities and companies[1], the Australian Government comprised 100[2] non-corporate Commonwealth entities (NCEs), 74 corporate Commonwealth entities (CCEs) and 16 Commonwealth companies (CCs); totaling 190 Australian Government entities, as of 30 June 2024.[3]

The information included in this report is primarily derived from the annual Australian Signals Directorate (ASD) Cyber Security Survey for Commonwealth Entities (hereafter 'the ASD survey'). In 2024, 94 per cent of all primary federal bodies participated in the survey, the highest participation rate to date. Data collected by ASD in the performance of its cyber security function supplements the ASD survey findings. While additional entities participated in the 2024 survey, this did not have a substantial impact on the overall findings of the report.

For the purposes of this report, an entity's cyber security posture is considered against the following criteria:

- Cyber security hardening: An entity's implementation of cyber security technical mitigations, primarily the Essential Eight mitigation strategies, to reduce the likelihood of an information and communications technology (ICT) system being compromised.[4]
- Incident preparedness and response: An entity's readiness to respond to a cyber security incident, and actions when a cyber security incident occurs.
- Leadership and planning: An entity's leadership engagement with cyber security and broader cyber security culture.

[1] Flipchart of the PGPA Act entities and companies, PGPA Act Flipchart and List

[2] The number of NCEs quoted excludes the Australian National Preventive Health Agency. This agency is listed on the PGPA Flipchart; however, it ceased operations in 30 June 2014, and is therefore excluded from all assessment described in this report.

[3] The total number of Australian Government entities increased from 189 at the end of the 2022-23 financial year.

[4] Find the Essential Eight at cyber.gov.au

Findings presented in this report indicate that, overall, Australian Government entities have established corporate governance mechanisms to understand their security risks and prepare for cyber threats. The findings also indicate required improvements in some areas and progress in others. In particular, the report finds that:

- The proportion of government entities that reached overall Maturity Level 2 across the Essential Eight mitigation strategies has declined. In 2024, 15 per cent of all entities reached overall Maturity Level 2, decreasing from 25 per cent in 2023.
- In 2024, 75 per cent of entities had a cyber security strategy, an increase from 73 per cent in 2023. Furthermore, 86 per cent of entities addressed cyber security disruptions in their business continuity and disaster recovery planning, an increase from 83 per cent in 2023.
- In 2024, 88 per cent of entities had a planned body of work to improve their cyber security, of which 82 per cent were funded.
- The majority of entities had planned for managing a cyber security incident, and were ready to respond if needed. In 2024, 86 per cent of entities had an incident response plan, an increase from 82 per cent in 2023.
- The proportion of entities that provided annual cyber security training to their workforce remained the same as in 2023, with 78 per cent providing this training in 2024. In 2024, 51 per cent of entities provided annual privileged user training, an increase from 39 per cent in 2023.[5]
- In 2024, 74 per cent of entities performed supply chain risk assessments for applications, ICT equipment and services. The percentage of entities reporting cyber security incidents to ASD remained low, with 32 per cent of entities indicating that they reported at least half of the cyber security incidents observed on their networks to ASD in 2024. ASD has some visibility and telemetry across Government agencies that assists with incident identification. ASD notified Australian Government entities 143 times of potential malicious cyber activity.

Legacy Information Technology (IT) presents significant and enduring risks to the cyber security posture of Australian Government entities and organisations. In April 2024, ASD published guidance on *Managing the Risks of Legacy IT*, which provides low-cost mitigations for legacy IT that government entities can draw upon, in addition to their own strategies.[6]

In order to improve their overall cyber security posture, it is recommended that entities:

- continue to implement the Essential Eight Mitigation strategies across their networks to at least Maturity Level 2
- increase cyber security incident reporting and share cyber threat information with ASD
- implement strategies for managing legacy IT now and into the future
- maintain an incident response plan, and exercise it at least every two years.

[5] Privileged user training is tailored to personnel with responsibilities beyond that of a normal user. Find the Guidelines for Personnel Security at cyber.gov.au

[6] Find the guidance to Managing the Risks of Legacy IT on cyber.gov.au

About this report

This report is prepared in response to a 2017 Joint Committee of Public Accounts and Audit (JCPAA) recommendation that ASD and the Attorney-General's Department (AGD) report annually to Parliament on the Commonwealth's cyber security.[7]

Under the *Protective Security Policy Framework* (PSPF), NCEs are required to respond to the survey, while CCEs and CCs are encouraged to participate. In 2024, all 100 NCEs responded to the ASD survey along with 79 CCEs and CCs, generating an overall completion rate of 94 per cent, the highest participation rate to date.

This report focuses on the 2024 ASD survey, while drawing on the 2022 and 2023 ASD surveys for comparison. Data collected by ASD in the performance of its cyber security function supplements the survey findings. For instance, metrics gathered by ASD's Cyber Hygiene Improvement Programs (CHIPs) scanning capability of internet-facing systems also provide updates on the implementation of effective cyber security standards and protocols.

This report does not identify entities by name. Any insight into the cyber security posture of individual entities made available to malicious cyber actors may increase the risk of those entities being targeted. All results have been anonymised and aggregated.

This report provides an assessment of the cyber security posture of entities as at 30 June 2024. It is the fifth such report to be tabled before Parliament.

[7] JCPAA Report 467: Cybersecurity Compliance, Report 467. For the report, see aph.gov.au. The reporting responsibility was transferred to the Department of Home Affairs on 3 August 2023.

The PSPF Assessment Report

As a response to the 2017 JCPAA's recommendation, NCEs must report on their security posture to their minister and the Department of Home Affairs. The 2022–23 PSPF Assessment Report refers particularly to the implementation of 16 government policies under the PSPF.[8]

Two policies specifically address cyber security posture:

- *PSPF Policy 10: Safeguarding data from cyber threats.* This addresses strategies to mitigate common and emerging cyber threats. Since 1 July 2022, Policy 10 requires entities to implement all 8 strategies of ASD's Essential Eight to Maturity Level 2 and consider if their threat environment warrants implementing Maturity Level 3.
- *PSPF Policy 11: Robust ICT systems.* This focuses on safeguarding ICT systems to support secure and continuous delivery of government business. It includes safeguarding ICT systems from cyber threats by effectively implementing principles from ASD's Information Security Manual (ISM).[9]

The PSPF Assessment Report is an aggregated assessment of how entities implement the PSPF policies and as such complements this ASD report. Some discrepancy between these results may be expected as the PSPF Report and the ASD survey use different assessment models to determine cyber security maturity. The PSPF report covering the 2023–24 financial year is expected to be published in early 2025.

On 1 November 2024, the Department of Home Affairs launched a new iteration of the PSPF. Future iterations of the PSPF Assessment Report will assess against any new or updated requirements introduced.

[8] Find the 2022–2023 PSPF Assessment Report at protectivesecurity.gov.au

[9] The ISM is a cyber security framework that entities can apply, using their risk management framework, to protect their information technology and operational technology systems, applications and data from cyber threat. Find the manual at cyber.gov.au

Cyber security hardening

Implementing technical cyber security controls helps entities defend their ICT environments against cyber security threats, thereby avoiding costly remediation, system downtime, lost productivity and loss of public confidence. This report refers to 2 measurements to assess government entities' implementation of technical cyber security controls:

- Responses to the ASD survey: Entities report on their progress implementing the controls recommended for each mitigation strategy, or a compensating control, which is then used to attain a corresponding Essential Eight maturity level.
- CHIPs results: CHIPs performs quarterly scans to detect key cyber hygiene indicators on entities' internet-facing systems and services, which are used to assess whether government entities are meeting cyber hygiene standards.

The Essential Eight

The Essential Eight outlines a set of 8 mitigation strategies designed to help entities reduce their vulnerability to cyber security incidents, and the impact of incidents if occurred.

The Essential Eight mitigation strategies are:

- Patch applications: Entities should apply patches for vulnerabilities that are released by vendors or alternative vendor mitigations in a timeframe appropriate to their exposure to the vulnerabilities. Increased emphasis has been placed on patching applications that routinely interact with untrusted content from the internet.
- Patch operating systems: Entities should apply patches for vulnerabilities or alternative vendor mitigations as soon as possible or in a timely manner within the constraints of system uptime requirements.
- Multi-factor authentication (MFA): Entities should use MFA, a security measure that requires 2 or more proofs of identity to grant access. A new minimum standard requires 'something users have', as well as 'something users know'.
- Restrict administrative privileges: Entities should limit the number of users with administrative privileges for operating systems and applications, as these users are able to make significant changes to system configuration and operation, bypass critical security settings and access sensitive data. Restricting administrative privileges makes it more difficult for malicious actors to elevate privileges, spread to other hosts, hide their existence, persist after reboot, obtain sensitive data or resist removal efforts.
- Application control: Entities should implement application control, a security approach designed to protect against malicious code (also known as malware) executing on systems. When implemented robustly, it ensures only approved applications can be executed.

- Restrict Microsoft Office macros: Entities should ensure that all macros are checked by assessors, who are independent of macro developers, to confirm that they are safe before being digitally signed or placed within trusted locations.
- User application hardening: Entities should remove unnecessary system applications and place restrictions on application functions that are vulnerable to malicious use.
- Regular backups: Entities should ensure there are regular backups of their systems and data as these will assist them recovering and maintaining operations in the event of cyber incidents.

The *Essential Eight Maturity Model* describes 4 maturity levels (0 to 3) for these strategies, which are determined based on the implementation of all the controls that ASD recommends, or appropriate compensating controls, for each strategy.

Higher levels of maturity are designed to defend against moderate-to-high degrees of sophistication in adversary tradecraft and targeting. As of 1 July 2022, the PSPF mandates that NCEs must implement all Essential Eight strategies to at least Maturity Level 2 and consider if their threat environment warrants implementing Maturity Level 3.[10]

ASD recommends that entities implement the Essential Eight mitigation strategies using a risk-based approach. When strategies cannot be fully implemented, compensating controls may be used to manage the residual risk. The controls must provide an equivalent level of protection to the specific Essential Eight requirements for which they are compensating.

Updates to Essential Eight

In November 2023, ASD made substantial updates to the Essential Eight Maturity Model. Key focus areas updated include patching timeframes, increasing adoption of phishing resistant MFA, supporting management of cloud services, and performing incident detection and response for internet-facing infrastructure. A complete list of these updates can be found at cyber.gov.au.

These updates address cyber security threats informed by the evolution of tradecraft used by malicious actors and ensure that ASD's cyber security advice remains contemporary, fit for purpose and commensurate with the threat. These updates are based on ASD's experience in producing cyber threat intelligence, responding to cyber security incidents, conducting penetration testing and assisting organisations to implement the Essential Eight mitigation strategies. They reduce the risk of compromise by malicious actors and limit its impact if compromise occurs.

Changes to the Essential Eight Maturity Model mean that entities which had not yet implemented new requirements would record a reduction in maturity level in comparison to 2023. This may account for the reduction in the percentage of entities meeting Maturity Level 2.

[10] Find out more at protectivesecurity.gov.au

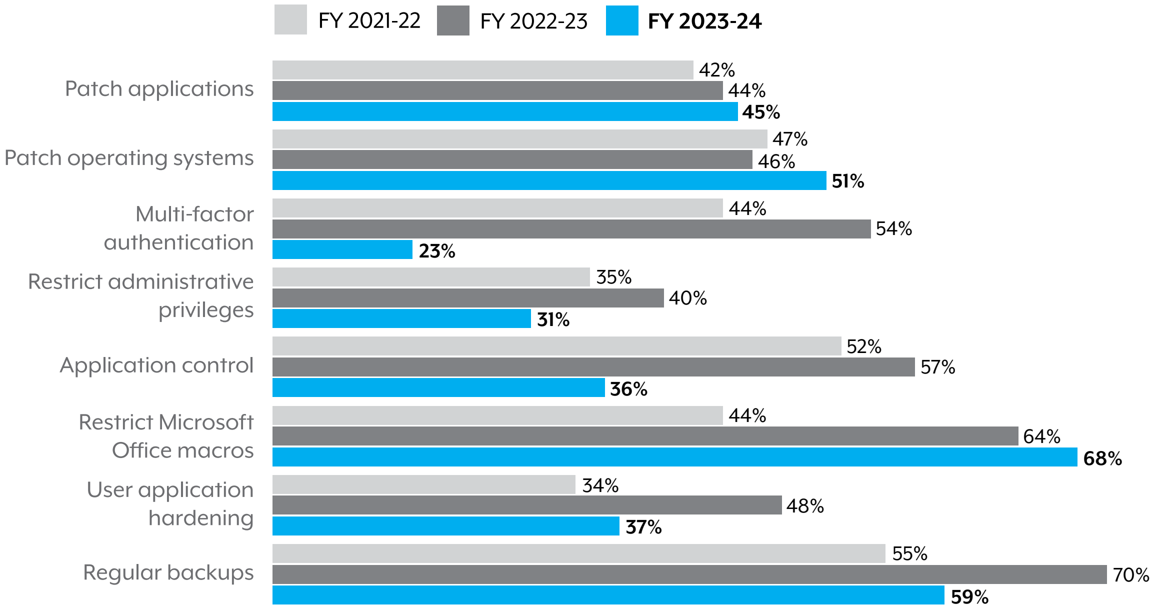
Implementing the Essential Eight

The mitigation strategies that constitute the Essential Eight are designed to complement each other and to provide coverage of various cyber threats. ASD recommends entities plan and implement controls to achieve at least the same maturity level across all 8 mitigation strategies. In order to achieve an overall Maturity Level, entities must at least meet that maturity level in each and every mitigation strategy. An entity's overall Maturity Level is equal to its least mature strategy.

According to the ASD survey, the proportion of entities that have achieved Maturity Level 2 across all 8 mitigation strategies remains low. In 2024, 15 per cent of all entities met Maturity Level 2, a decrease from 2023, when 25 per cent of all entities met Maturity Level 2.

At the mitigation strategy level, there is a considerable range in the percentages of entities that achieved Maturity Level 2 or higher for each strategy. For 3 of the 8 mitigation strategies, more than half of the entities achieved Maturity Level 2. For the remaining 5 mitigation strategies, the proportion of entities that reached Maturity Level 2 vary between 23 per cent and 45 per cent.

FIGURE 1: Entities that reached Essential Eight Maturity Level 2 or higher.



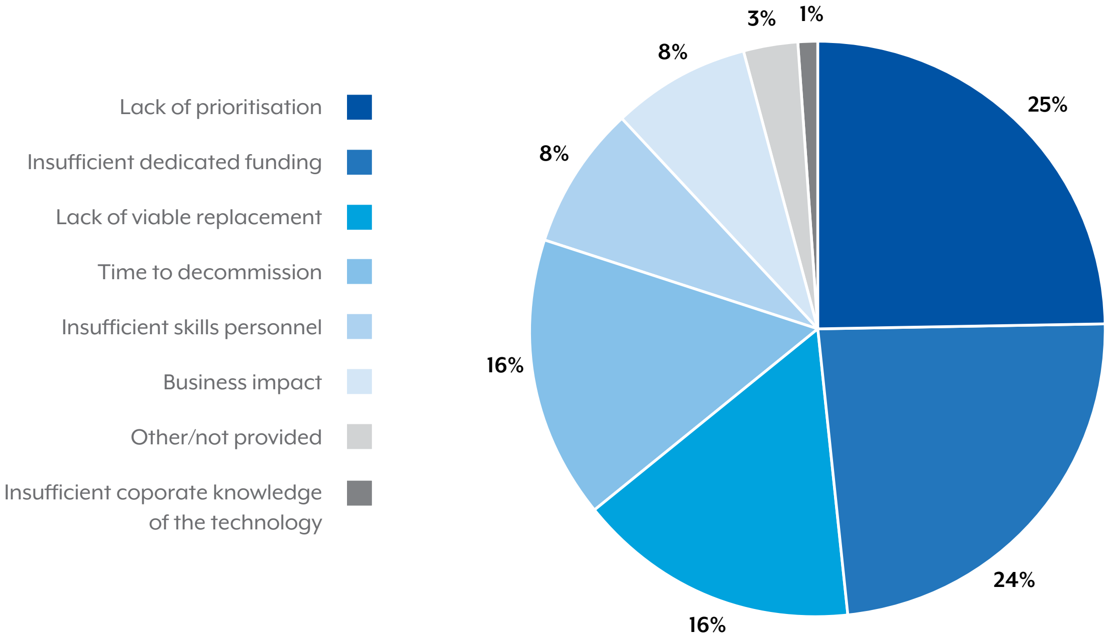
Legacy IT and the Essential Eight

The use of legacy IT within a system can inhibit implementing the Essential Eight. Legacy IT is more vulnerable to cyber attacks as vendors do not support the development of security updates, or limit security services. Malicious actors may be able to compromise legacy IT, and use it to gain access to more modern systems in IT environments. As such, legacy IT presents significant and enduring risks to the cyber security posture of Australian Government entities.

Legacy IT can prevent Australian Government entities achieving Maturity Level 2. In 2024, 71 per cent of entities indicated that the use of legacy technologies had impacted their ability to implement the Essential Eight, an increase from 52 per cent of entities in 2023. Entities reported that the most significant reason for continued use of legacy IT was a lack of prioritisation to decommission, and a lack of dedicated funding. Where legacy systems cannot immediately be replaced, ASD provides guidance on mitigating the risks posed by legacy IT.

In 2024, ASD released guidance setting out low-cost mitigations for legacy IT that organisations can draw upon, in addition to their own strategies.[11]

FIGURE 2: Entities' reported most significant reason for using Legacy IT



[11] Managing the Risks of Legacy IT Practitioner Guidance at cyber.gov.au

CASE STUDY: Joint services for high priority entity

In July 2023, ASD conducted the first joint Cyber Maturity Measurement Program (CMMP) and Critical Infrastructure Uplift Program (CI-UP) assessment of a high-priority government entity. Conducting the CMMP and CI-UP assessments concurrently allowed for minimal disruption to the entity while identifying cyber security uplift opportunities for both its information technology and operational technology (OT) environments.

ASD identified 20 critical findings and provided 10 priority recommendations related to specific vulnerabilities and weaknesses as part of the assessment. A further 90 uplift opportunities related to the Essential Eight, and general cyber security and OT security posture hardening were recommended.

The entity was engaged and motivated throughout the assessment, working with ASD to improve its cyber security posture by quickly and effectively remediating the critical vulnerabilities and weaknesses identified. As a result of these remediations, the entity was able to successfully improve its cyber security posture, making it more difficult for malicious actors to compromise its systems.

Cyber Hygiene Improvement Programs (CHIPs)

Under CHIPs, ASD systematically scans domains and servers of Australian Government entities to find indicators of effective cyber security standards and protocols, including effective use of:

- security protocols on email domains[12]
- encryption on email servers[13]
- encryption on web servers.[14]

CHIPs scans also identify whether the government entities' websites are being actively maintained and whether their servers are running end-of-life software or are otherwise unsupported.[15]

This report addresses the proportion of:

- domains or servers that have implemented recommended minimum security measures across federal government networks overall
- Australian Government entities that have implemented those measures across at least 90 per cent of their servers or domains. This is considered 'effective' implementation for each protocol.

The number of domains and servers managed by a given entity varies significantly. As such, an increase or decrease in the number of domains or servers implementing a given security measure is often not reflected at the entity level.

CHIPs results from May 2023 and May 2024

Across all servers and domains, the implementation of effective email domain security protocols and effective email encryption increased in 2024, as did the proportion of actively maintained websites. However, implementing effective website encryption decreased slightly.[16]

Between 2023 and 2024, the proportion of government entities implementing effective email domain security and actively maintaining their websites increased. The proportion of entities implementing effective website encryption remained the same, while the proportion of entities implementing effective email encryption decreased.

[12] The minimum recommended email security protocols on domains is, 'The domain has a valid DMARC record, or has a valid DMARC record on its base domain, with an effective policy of 'reject' or 'quarantine'.'

[13] The minimum recommended email encryption is, 'The website sends an HSTS header when accessed and HTTPS is enabled and no weak or insecure cipher suites are used and users are redirected to an HTTPS connection and the oldest supported version of TLS is 1.2 or higher and client – initiated.'

[14] The minimum recommended web server encryption is, 'The mail server supports Opportunistic TLS (STARTTLS) and supports at least TLS 1.2 (but may also allow TLS 1.1 and TLS 1.0 for backwards compatibility) and has a valid certificate and offers at least one strong cipher and offers no insecure ciphers.'

[15] The minimum recommended website maintenance is, 'Running supported applications, has a valid certificate and handles requests appropriately.'

[16] In 2024, CHIPs enhanced their data collection methodology to provide more accurate year-on-year figures. This enhanced methodology has been backdated and has resulted in minimal variations from the data provided in the Commonwealth Cyber Security Posture in 2023 report.

FIGURE 3: Implementing email domain security protocols

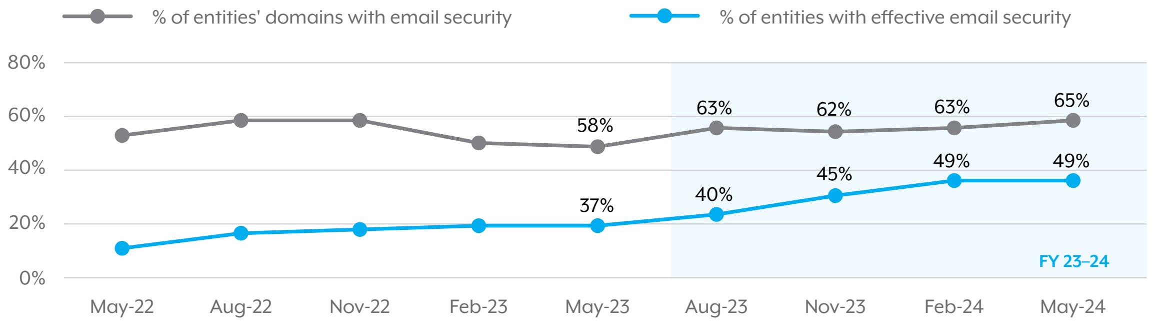


FIGURE 4: Implementing email encryption

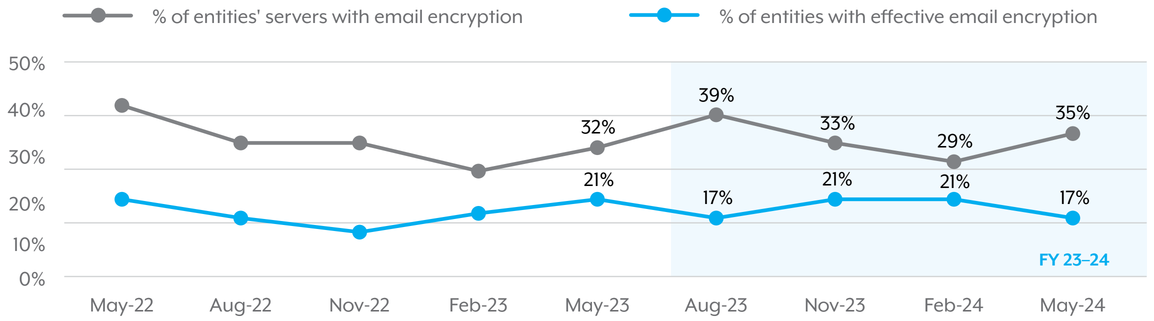


FIGURE 5: Implementing website encryption

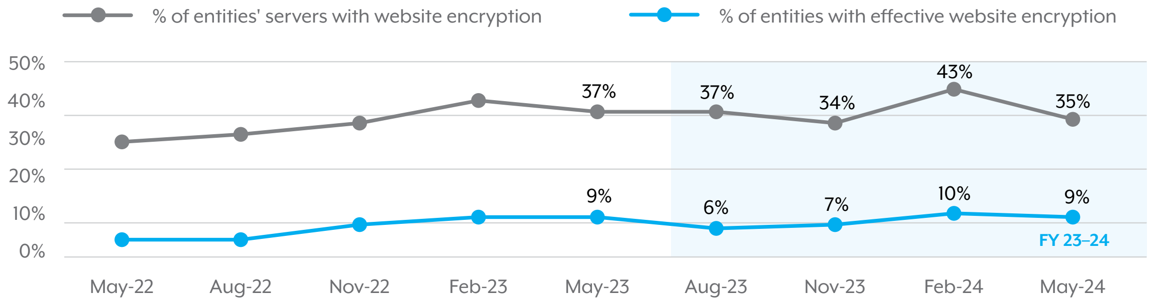
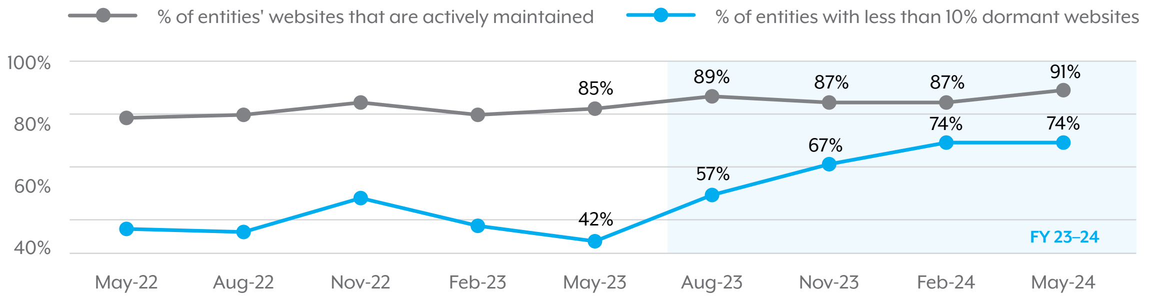


FIGURE 6: Actively maintained websites



CASE STUDY: Australian Government and CitrixBleed

Since August 2023, threat actors across the world have attempted to exploit a specific vulnerability in the remote desktop application Citrix. A common vulnerability, known as CitrixBleed, allows threat actors to bypass password requirements and MFA in order to access legitimate user sessions on Citrix.

When ASD became aware of this vulnerability, potential exposure across the Australian economy was identified through CHIPs scanning capability. ASD scans revealed CitrixBleed had not yet been exploited in government networks.

ASD publicly released mitigation strategies, technical advice and guidance for detecting and mitigating CitrixBleed. ASD's actions included producing a joint public technical advisory on mitigations for CitrixBleed with the US's Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, and Multi-State Information Sharing and Analysis Centre.

ASD scanning plays a critical role in understanding the changing cyber threat environment. Identifying vulnerabilities early improves timely patching of applications and operating systems by government entities.

Incident preparedness and response

The Australian Government is a common target for malicious cyber activity. In the 2023–24 financial year, ASD responded to 406 cyber security incidents reported by Australian Government entities. Reports from the Australian Government represented 36 per cent of all cyber security incidents responded to by ASD. This is an increase from the 2022–23 financial year where, when ASD responded to 348 Australian Government reports, representing 31 per cent of all cyber security incidents.

Cyber security events and cyber security incidents are defined in the ISM, as follows:

- A cyber security event is an occurrence of a system, service or network state indicating 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 either has compromised business operations or has a significant probability of compromising business operations.

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

Implementing incident preparedness and reporting

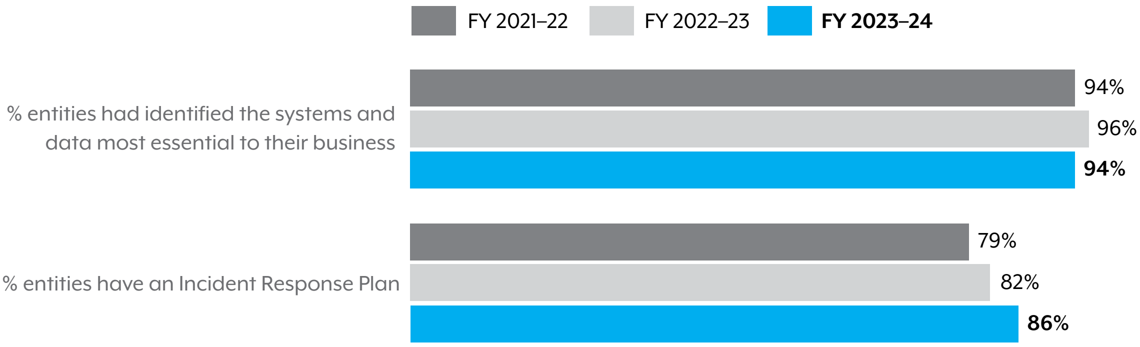
An entity's cyber resilience is based on its ability to detect and manage cyber security events, and the capacity to adapt to disruptions caused by cyber security incidents while maintaining continuous business operations.

The ASD survey included questions designed to assess entities' levels of preparedness to respond to a cyber security incident, their cyber event and incident detection capabilities and their incident reporting behaviours.

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.

Responses to the survey indicate that 94 per cent of entities had planned for a cyber security incident, and 86 per cent of entities were ready to respond if needed, as shown in Figure 7.

FIGURE 7: Indicators of entities' cyber security incident preparedness



Developing, implementing and maintaining a cyber security incident register can assist with ensuring that appropriate remediation activities are undertaken in response to cyber security incidents. In addition, the types and frequency of cyber security incidents, along with the costs of remediation activities, can be used to inform future risk assessment activities.

Implementing a centralised event logging capability system enables incident aggregation, selection and analysis. In 2024, 89 per cent of entities had a centralised logging capability system.[17]

CASE STUDY: Security Incident and Event Management (SIEM) and Security, Orchestration, Automation and Response (SOAR) Capability Uplift Pilot Program

In 2023–24, ASD commenced a SIEM/SOAR Pilot Program, utilising a repeatable methodology to establish or improve participating entities' cyber visibility capability, supported by the provision of professional services, limited licensing, and access to vendor-specific training.

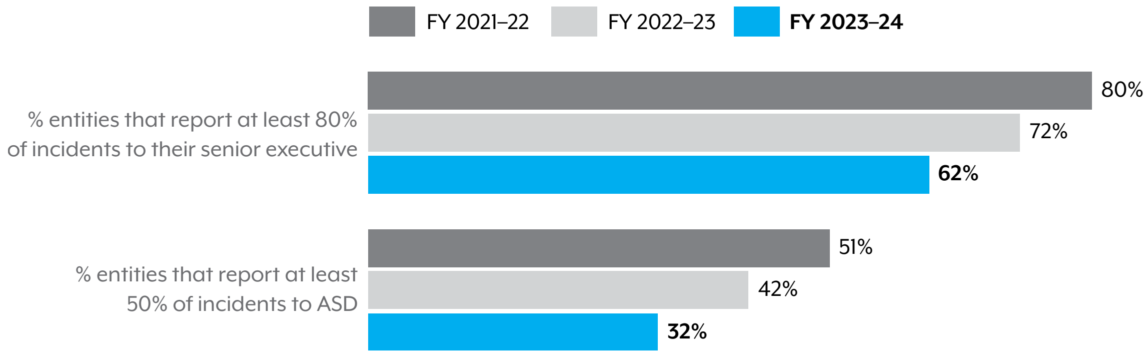
Entities with no previous capabilities were able to establish visibility of up to 93 per cent of their ICT environments. Total active SIEM detections increased by 51 per cent across all entities.

The program also improved workforce skills, with 180 staff participating in bespoke training. All participating agencies increased the number of people with foundational cyber security knowledge. Outside of the participating agencies, 428 staff from across the Australian Government engaged in recommended training.

It is essential that entities report cyber security incidents to ASD, to ensure those incidents are dealt with appropriately and that any impact is fully considered.

[17] Previous editions of the ASD survey asked entities to report whether they used a security information and event management platform (SIEM).

FIGURE 8: Indicators of entities' cyber security incident reporting



Under PSPF Policy 5, entities are required to report 'significant or reportable' cyber security incidents to ASD. The low rate of reporting may be due to a proportion of entities experiencing a high number of low-impact incidents, which do not meet the PSPF reporting threshold. ASD has almost complete coverage of the internet-facing connected systems of all government entities through CHIPs reporting, allowing for rapid identification of cyber security vulnerabilities. The Host Based Sensor Program and the Gateway Sensor Program Network also provide visibility of cyber security incidents and the security posture of Australian Government ICT systems.

The Annual Cyber Threat Report 2024 notes that the Federal Government has the highest reporting rate for cyber security incidents across the Australian economy.

ASD maintains a national cyber threat picture informed by reporting of cyber security incidents by Australian Government entities and private entities. Aggregating cyber security incident data enables ASD to provide threat mitigation advice with the latest trends and threats posed by malicious cyber actors. Any degradation in the quantity or quality of information reported to ASD reduces ASD's capacity to mitigate the impacts of cyber compromise.

Leadership and planning

Strong leadership is essential in setting and maintaining a positive cyber security culture, and ensuring that cyber security remains part of an entity'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 briefing senior leadership on the entity's cyber security program and ensuring compliance with cyber security policy, standards, regulations and legislation.

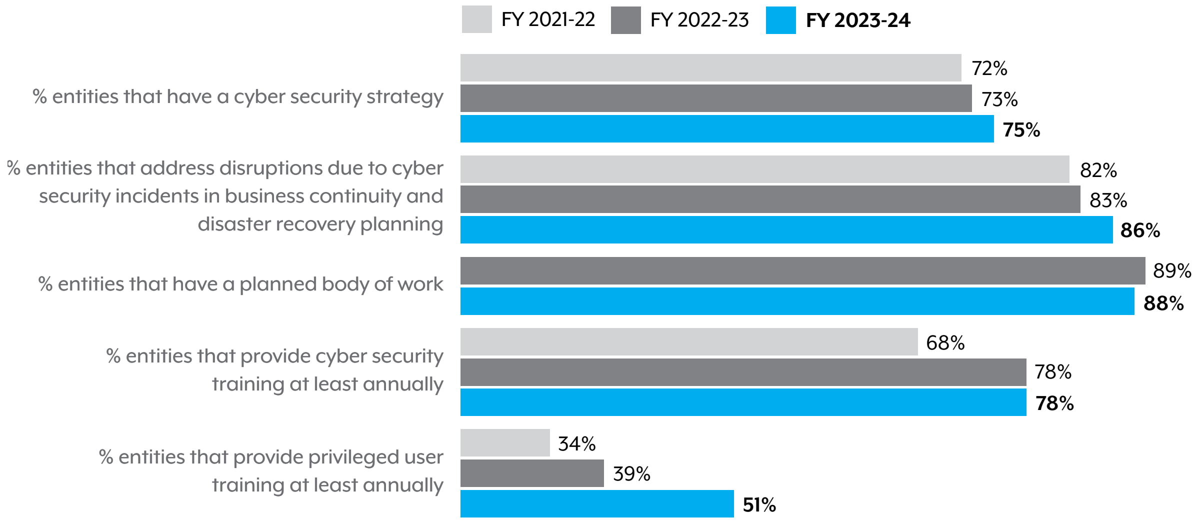
The broader workforce also plays a key part in maintaining cyber security, and entities should provide ongoing cyber security awareness training to all personnel to help them best understand their cyber security responsibilities.

Implementing leadership and planning

Entities were assessed through a series of ASD survey questions designed to provide indications of their cyber security leadership, planning and overall culture.

Over the 2023–24 financial year, survey responses indicated improvement in cyber security leadership and planning, as shown in Figure 9.

FIGURE 9: Indicators of entities' leadership and planning



In 2024, 75 per cent of entities reported having a cyber security strategy, an increase from 73 per cent in 2023. A cyber security strategy articulates an entity's plans and priorities for cyber security uplift and mechanisms to manage cyber security risks. Achieving and maintaining effective cyber security mitigations requires investment, sufficient capability and clear objectives.

The cyber security posture of government entities is affected by the risks associated with cyber supply chains. To mitigate potential increase to their security risk profile, government entities should conduct risk management activities and risk assessment for each component of their supply chain.[18] In 2024, 74 per cent of entities reported having performed supply chain assessments for suppliers of applications, ICT equipment and services in order to assess potential impact to their system's security risk profiles.

In an effort to uplift cyber resilience, government entities participated in ASD's Cyber Security Partnership Program.[19] In 2024, 148 Australian Government entities participated in the program, an increase from 133 government entities in 2023.

Under the PSPF, Direction 003-2024 on *Supporting Visibility on the Cyber Threat*, published on 8 July 2024, participation in the program is now mandatory for NCEs. By 30 June 2024, 96 per cent of NCEs had joined the program.

[18] This may include application services, authentication services, backup services, desktop services, enterprise mobility services, gateway services, hosting services, network services, procurement services, security services, support services, and many other business-related services.

[19] ASD's Cyber Security Partnership Program enables Australian organisations and individuals to engage with ASD and partners to lift cyber resilience across Australia. See the Cyber Security Partnership Program at cyber.gov.au

CASE STUDY: Effective management of a phishing incident

In late February 2024, an Australian Government entity reported an on-going phishing email campaign to ASD.

Almost 80 of the entity's mailboxes were targeted over a three-hour period. As some of these mailboxes were linked to distribution lists, there were around 500 recipients overall. Due to the emails having unique senders, subjects and attachments, more than half were not identified as suspicious by the entity's email security gateway.

The entity's cyber operations team suspected the phishing emails were likely carrying PikaBot malware. PikaBot is known for email thread hijacking, in which a malicious payload is distributed by gaining access to an existing email conversation.

While a small number of the entity's employees opened the email attachment, the resulting network connections were blocked by firewall rules. Meanwhile, a large number of employees correctly identified and internally reported the emails as phishing attempts. The cyber operations team contained the incident by blocking the malicious senders, files, domains and purging the delivered emails.

The attack campaign was unsuccessful due to layered security controls, organisational security culture and the entity's incident response capability.

Prompt reporting to ASD also helps identify trends in targeting. At the same time as this incident, 2 other government departments reported PikaBot phishing email campaigns. The reporting enables ASD to produce timely tailored advice and update key cyber security guidance such as the ISM.

Conclusion

The findings presented in this report indicate that entities' cyber security postures were well-established in some areas, and required improvement in others. In particular:

a. The proportion of government entities that had reached overall Maturity Level 2 across the Essential Eight mitigation strategies had decreased.

b. Between 2023 and 2024, the proportion of government entities applying effective email domain security improved, as did the proportion of entities hosting only valid websites on their web servers, as measured by ASD’s CHIPs. However, the proportion of government entities applying effective email encryption decreased. The proportion of entities applying effective website encryption remained consistent.

c. The majority of entities had planned for a cyber security incident, and were ready to respond if needed.

d. The percentage of entities reporting cyber security incidents to ASD had declined over the 2023–24 financial year.

e. Indicators of cyber security leadership and planning had remained high, and showed improvement across entities.

f. The proportion of entities that provided annual cyber security training to their workforce remained consistent in 2023–24 financial year, while the proportion of entities providing Privileged User Training to their staff annually increased.

Report to Parliament 2025

The *Commonwealth Cyber Security Posture in 2025* report to Parliament will be delivered by November 2025.

ASD services supporting Australian Government cyber security

Cyber security hardening

Cyber security maturity assessment and uplift

ASD's Cyber Maturity Measurement Program (CMMP) assessments involve teams of technical subject matter experts working with government entities to assess their cyber security maturity against the Essential Eight, as well as assessing their broader cyber security posture. Entities are provided with a detailed report containing tailored advice and recommendations to improve their cyber security maturity.

The Cyber Uplift Remediation Program (CURP) is an enabler for high-priority Australian Government entities to improve their cyber security posture. The objective of CURP is to uplift Essential Eight maturity, improve cyber security posture, and remediate other cyber security vulnerabilities for government entities. In partnership with government entities, CURP provides skilled technical specialists who help implement security controls and provide further recommendations aligned with ASD's findings. They also provide advice and services through complementary offerings.

In the 2023–24 financial year, ASD:

- carried out 14 CMMP assessments with high-priority government entities, an increase from 5 assessments in the previous financial year
- provided 17 CURP uplift services for high-priority government entities to improve their cyber security hygiene, awareness and implementation of a security roadmap, an increase from 13 uplifts in the previous financial year.

Cyber Hygiene Improvement Programs

CHIPs is an open-source intelligence capability that analyses the cyber posture and hygiene of internet-facing systems and assets for government and critical infrastructure to identify cyber security vulnerabilities. CHIPs aims to improve Australia's cyber security through building capabilities to provide a strategic advantage against threat actors. CHIPs provides quarterly reports to entities, detailing their vulnerabilities and providing network owners with actionable information to inform cyber security posture improvement activities. The program relies on a mixture of open-source, commercial and directly collected data to provide situational awareness to ASD.

High-Priority Operational Tasking Cyber Hygiene Improvement Programs

The High-Priority Operational Tasking (HOT) CHIPs capability enables vulnerability assessment and triage with targeted data collection in response to critical vulnerabilities with Australian interests. The HOT CHIPs scans build ASD's visibility of particular cyber security vulnerabilities across the Australian economy and offer network owners highly targeted, timely and actionable steps that can be employed to identify, reduce, and mitigate system compromise.

During the 2023–24 financial year, ASD performed 365 HOT CHIPs assessments, up from 100 in the 2022–23 financial year.

Active Vulnerability Assessments

ASD's Active Vulnerability Assessments (AVA) capability identifies security vulnerabilities that may be used by a sophisticated cyber security actor. An AVA is a long-term engagement with high-priority customers to simulate the presence of a sophisticated cyber adversary while remaining undetected on the customer's network. The outcome of the AVA activity allows customers to understand their vulnerabilities, and test their responses when they detect unusual activity.

Hunt

ASD proactively conducts cyber threat hunt activities on priority Australian networks to detect unnoticed intrusions by sophisticated cyber actors. This service is offered to high-priority entities, including in support of events of national significance.

In the 2023–24 financial year, ASD conducted 2 hunt activities on priority government networks.

Sensor programs

The Host Based Sensor (HBS) Program and the Gateway Sensor Program Network (GSPN) provide visibility of the cyber security posture of Australian Government ICT systems by collecting telemetry data from government devices. These programs allow ASD to help entities identify weaknesses in their cyber security, detect intrusions on their ICT infrastructure, and mitigate the consequences of compromise.

In the 2023–24 financial year, ASD supported 7 additional Australian Government entities to join the HBS program, bringing the total number of entities to 45.

The GSPN program has a total of 63 Australian Government entities subscribed.

Incident preparedness and response

Alerts and advisories

ASD publishes alerts and advisories on cyber.gov.au to inform Australians about cyber security threats and mitigations. ASD Alert Service is a subscription-based email service that informs Australians about the latest threats and vulnerabilities, and how to address risks on their devices and computer networks.

Australian Cyber Security Hotline

The Australian Cyber Security Hotline '1300 CYBER1' (1300 292 371) provides advice and assistance to Australians and entities impacted by cyber security incidents. The hotline is available 24 hours a day, 7 days a week.

National Exercise Program

The National Exercise Program (NEP) works in partnership with Australian critical infrastructure and government to scope, plan, deliver and evaluate cyber security exercises to improve Australia's overall cyber resilience. The NEP also delivers exercise management training workshops for Australian critical infrastructure and government.

In the 2023–24 financial year, ASD delivered 16 exercises for Australian critical infrastructure and government.

Incident response

ASD's incident management capabilities provide tailored incident response advice and guidance to Australians impacted by a cyber security incident. For nationally significant incidents, ASD may also provide incident investigation support. ASD is not a law enforcement entity or regulator; however, it does work closely with these entities if needed.

Cyber Threat Intelligence Sharing

Cyber Threat Intelligence Sharing (CTIS) allows participating entities to share observable indicators of compromise (IOCs) at machine-to-machine speed. Participating entities can use these IOCs to identify activity on their own networks. The CTIS platform also allows participating entities to share the IOCs observed on their own networks with other CTIS partners.

By June 2024, 33 Australian Government entities had joined the program, an increase from 24 entities in June 2023.

Under the PSPF, Direction 003-2024 on *Supporting Visibility on the Cyber Threat*, published on 8 July 2024, mandates that NCEs using threat intelligence sharing platforms share cyber threat information with ASD.[20]

[20] See the PSPF Direction 003-2024 at protectivesecurity.gov.au

Australian Protective Domain Name System

The Australian Protective Domain Name System (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.

By June 2024, 49 Australian Government entities had subscribed to AUPDNS, an increase from 39 entities in June 2023.

Leadership and planning

ASD's Cyber Security Partnership Program

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

Under the PSPF, Direction 003-2024 on *Supporting Visibility on the Cyber Threat*, published on 8 July 2024, mandates NCEs to participate in ASD's Cyber Security Partnership Program.[21]

An ASD Network Partnership is available to organisations with responsibility for the security of a network or networks (either their own or on behalf of customers) as well as academic, research and not-for-profit institutions with an active interest and expertise in cyber security.

[21] See the PSPF Direction 003-2024 at protectivesecurity.gov.au

ASD.GOV.AU