THE COMMONWEALTH CYBER SECURITY POSTURE IN 2019

REPORT TO PARLIAMENT

March 2020

CONTACT DETAILS

Phone
Media enquiries: asd.assist@defence.gov.au
Cyber Security Hotline: 1300 CYBER1 (1300 292 371)

Website
www.cyber.gov.au
Location of this report www.cyber.gov.au

Contact
Feedback about this Report is welcome and should be directed to:

ASD Assist
Email: asd.assist@defence.gov.au
Postal: Australian Signals Directorate
Brindabella Park
PO Box 5076
KINGSTON ACT 2604

Introduction

Throughout 2019, a range of malicious cyber actors continued to target Australia, conducting persistent cyber operations that threatened Australia's security, stability and prosperity.

Cyber operations were often sophisticated, and deliberately targeted Australia in order to obtain information on: defence capabilities; cutting-edge Australian research; valuable intellectual property; and the personal information of Australian residents and Government staff. These threats had the potential to affect the ability of the Australian Government to effectively serve the public and keep their trust.

The Australian Cyber Security Centre (ACSC) within the Australian Signals Directorate (ASD) leads the Australian Government's operational cyber security capability. The ACSC brings together cyber security capabilities from across the Australian Government to provide cyber security advice and assistance to Commonwealth entities, state and territory and local governments, businesses, academia, and individuals.

The ACSC monitors cyber threats targeting Australian interests and, when a serious cyber incident occurs, leads the Australian Government's response: providing advice and assistance to remediate and mitigate the threat and strengthen our nation's defences.

The ACSC's cyber security advice on how to prevent and respond to incidents can be found on cyber.gov.au. At the centre of the ACSC's advice is the *Strategies to Mitigate Cyber Security Incidents*[1]. While no single mitigation strategy can comprehensively prevent cyber security incidents, the eight mitigation strategies with an effectiveness rating of 'essential' are considered the cyber security baseline for all organisations to protect their systems against a range of cyber adversaries. These eight strategies are known collectively as the *Essential Eight*[2]. The ACSC recommends entities aim to achieve Maturity Level Three for each of the *Essential Eight* – meaning the entity should be fully aligned with the intent of each mitigation strategy[3].

The *Protective Security Policy Framework* (PSPF), administered by the Attorney-General's Department (AGD) mandates that all non-corporate Commonwealth entities[4] implement the first four mitigation strategies (known as the *Top Four*) – and strongly recommends the adoption of the entire *Essential Eight*. Entities must also consider other strategies included in the ACSC's *Strategies to Mitigate Cyber Security Incidents*.

Individual Commonwealth entities retain responsibility for maintaining the confidentiality, integrity and availability of their information. Cyber security maturity is a compliance and risk management issue for each accountable authority to

[1] Further information on the *Strategies to Mitigate Cyber Security Incidents* can be found at https://www.cyber.gov.au/publications/strategies-to-mitigate-cyber-security-incidents.

[2] Further information on the *Essential Eight* can be found at: https://www.cyber.gov.au/publications/essential-eight-explained.

[3] Further information on the *Essential Eight Maturity Model* can be found at: https://www.cyber.gov.au/publications/essential-eight-maturity-model.

[4] As defined in the *Public Governance, Performance and Accountability Act 2013*, section 11 (b).

balance in the context of their unique risk environments and the complexities of their operations.

To support the Australian Government's awareness of the overall cyber threat environment – and the continual recalibration of cyber security measures – Commonwealth entities are required to self-assess their implementation of the *Essential Eight* and report annually to both the ASD and AGD. The Department of Home Affairs supports ASD and AGD to then drive the improvement of cyber security standards across Government, helping to ensure Commonwealth entities increase their cyber security maturity to address their individual risk profiles.

The Joint Committee of Public Accounts and Audit (JCPAA) recommended that ASD and AGD report to Parliament annually on the Commonwealth's cyber security posture. The Australian Government agreed to this recommendation in April 2019 in order to support increased transparency in cyber security reporting. This is the first such annual Report.

Identifying the cyber security posture or vulnerabilities of individual Commonwealth entities may increase their risk of being targeted by malicious cyber actors. This Report, therefore, does not identify specific entities – all data has been anonymised and provided in aggregate.

This Report is based on information held by ASD and AGD from 2019. Therefore the information can only indicate the maturity of an entity's cyber security posture at the time it was provided — and is specific to the unique circumstances of that entity, at that time. However, with the cyber threat constantly evolving, and Commonwealth entities continually updating their security measures in response, the overall Commonwealth cyber security posture remains fluid.

It is important to note that no one entity – including ASD and AGD – has full oversight or visibility of the cyber security posture of all Commonwealth entities, due to the fact that each entity is responsible for the security of their own network. The findings in this Report are, therefore, limited to information obtained through the *ACSC Cyber Security Survey* and the 2018–19 PSPF maturity reporting, combined with the results of the whole-of-government *Cyber Uplift for Federal Government Systems and for the 2019 Federal Election* Budget measure (Cyber Uplift) and cyber security incident reporting and investigations. Some of the information is self-reported and, therefore, cannot be independently verified.

Australian Government cyber security initiatives in 2019

Throughout 2019, the Australian Government continued its work to establish effective cyber security behaviours and increase the overall cyber security of Commonwealth entities.

Cyber Uplift

In mid-2019, the Australian Government expanded ACSC assistance to entities – through the whole-of-government *Cyber Uplift for Federal Government Systems and for the 2019 Federal Election* Budget measure (Cyber Uplift) – to strengthen the cyber security of Australian Government networks through enhanced technical guidance, improved verification, and increased transparency and accountability.

The Cyber Uplift included ACSC teams conducting 'sprint' programs to assess and baseline the maturity of 25 Commonwealth entities in implementing the *Essential Eight*. Importantly, these ACSC sprint teams were also able to identify and support these 25 entities in implementing additional measures to strengthen their cyber security posture. This included providing technical advice, services and tools, in order to remediate identified vulnerabilities (see Case Studies 1 and 2). Each entity received tailored advice and guidance, which provided a snapshot of their maturity level, as well as prioritised recommendations and a roadmap for future improvements to their cyber security maturity.

Case Study 1

During the Cyber Uplift sprints, a misconfiguration of an entity's data backup system was identified. This made it vulnerable to a potential ransomware attack against its backup data. Through the Cyber Uplift sprint process the entity was able to remediate the vulnerability, increasing its backup data maturity level and ensuring it was better protected against any future ransomware attack on its backup system – and could quickly restore its systems and data.

Another important outcome of the Cyber Uplift was the creation of an ongoing forum for Chief Information Officers and Chief Information Security Officers from across the Australian Government (the CIO/CISO Forum). The ACSC established the CIO/CISO Forum in July 2019 and continues to use this forum to share the information gained from the Cyber Uplift sprints, including with entities who were not included in the original sprint programs.

Case Study 2

During the Cyber Uplift sprints, it was discovered that an entity had not been able to properly implement application whitelisting for workstations and servers. To fix this issue, the entity integrated a template containing hardened application whitelisting configurations to prevent unauthorised code execution on their systems. This resulted in an increase in their cyber security maturity.

The CIO/CISO Forum complements AGD's existing Chief Security Officer Forum and enables senior departmental officials responsible for cyber security to share the collective knowledge and experience of all members. This helps to improve the cyber security posture of individual entities – and the overall Commonwealth cyber security posture.

The CIO/CISO Forum is complemented by a digital newsletter and technical drop-in opportunities within the ACSC, to enable entities to stay across the latest changes in the cyber security threat environment.

A Cyber Security Response Fund was also established to provide funding to manage critical whole-of-government cyber risks and any significant cyber incidents. This includes providing training to improve cyber security as well as tailored services based on the findings from the Cyber Uplift sprints.

The Cyber Uplift also included the ACSC trialling strategic host-based sensors with two Commonwealth entities, covering approximately 10,000 hosts. These sensors provided the ACSC and the entities themselves with data to identify malicious cyber activities, generate threat indicators and contribute to the development of mitigation strategies. In addition, the Digital Transformation Agency developed a suite of Microsoft Office 365 productivity tools, including secure desktops and workspaces, with enhanced security arrangements.

The Cyber Uplift has improved the ACSC's visibility of vulnerabilities on Australian Government networks, created a network of government CIOs and CISOs, increased general cyber security expertise and awareness across Commonwealth entities, and enabled entities to rapidly implement mitigations to protect against identified vulnerabilities. The Cyber Uplift has been an important foundation for the Australian Government's effort to strengthen Government systems and networks and has helped the ACSC to tailor advice and assistance to Commonwealth entities.

Electoral Integrity Assurance

In April 2019, the Electoral Integrity Assurance Taskforce (the Taskforce) was convened to consider matters of electoral integrity in the 2019 Federal Election. In the period leading up to the election, the Taskforce was hosted at the ACSC. This joint-agency collaboration was formed to support agencies to use their authority and capability to proactively identify, analyse and respond to (where appropriate) incidents that could undermine the integrity of the 2019 Federal Election. The potential scope of activity included malicious cyber activity, electoral fraud, foreign interference, and disinformation campaigns.

The ACSC was an integral member of the Taskforce, which was co-led by the Department of Finance and the Australian Electoral Commission (AEC). Members of the Taskforce worked together to consider matters that may have impacted on the integrity of the outcome of the 2019 Federal Election, including consideration of the security of the AEC's networks and online systems.

Activation of the Cyber Incident Management Arrangements

The ACSC provides the secretariat for the National Cyber Security Committee (NCSC) and coordinates the activation of Australia's Cyber Incident Management Arrangements (CIMA)[5]. In 2019, the ACSC coordinated three CIMA activations in response to:

- the compromise of the Department of Parliamentary Services' network in a cyber intrusion that also affected the networks of the major political parties

[5] Australia's Cyber Incident Management Arrangements outline inter-jurisdictional coordination arrangements, roles and responsibilities, and principles for cooperation in response to national cyber incidents.

- the BlueKeep vulnerability that affected unpatched older versions of Windows operating systems
- the Emotet malware campaign.

The activation of these arrangements put all government entities – Commonwealth, state and territory – on heightened alert, with entities actively monitoring and defending their networks from the identified threat, based on advice from the ACSC.

National Exercises

The National Exercise Program helps validate and strengthen Australia's nation-wide cyber security arrangements by helping Commonwealth entities review and test their cyber incident response plans. This helps ensure entities can respond effectively to – and recover quickly from – a cyber incident.

In 2019, the ACSC assisted with nine cyber security exercises that involved eight Commonwealth entities. These exercises: improved command, control and coordination of cyber security incidents within Commonwealth entities; helped broaden the understanding of roles and responsibilities within and across governments and industry; and increased cyber security expertise across the Australian Government.

Cyber Hygiene Improvement Programs

The Cyber Hygiene Improvement Programs (CHIPs) involves a series of campaigns to improve the cyber security posture of Commonwealth, state and territory government entities. CHIPs has visibility of, and is tracking, cyber hygiene indicators across approximately 18,000 Australian Government domains. This provides entities with data-driven, actionable information to guide their cyber security efforts.

In 2019, CHIPs campaigns focused on the use of encryption on government websites and combatting fake emails. These campaigns resulted in a sizable increase in the number of Australian Government domains with adequate protection against fake emails and a decrease in the number of domains without encryption.

Cyber skills

In 2019, in order to increase digital skills across the Australian Public Service, the Digital Transformation Agency worked closely with ASD and other Commonwealth entities to develop the Information Security stream of the *Digital Career Pathways*. The *Digital Career Pathways* provides APS employees with guidance on how they can use their existing information and communications technology (ICT) skills in other roles and what new skills they might need in order to excel in those roles. The ASD *Cyber Skills Framework* – ASD's first publicly available skills framework defining the skills and proficiency levels of nine cyber security roles – was also released in 2019 and supports the four Information Security stream career pathways: Analysis; Architecture; Operations; and Testing.

Cyber incident investigations

ACSC responses to, and investigations of, cyber security incidents also help to increase the cyber security of Commonwealth entities. As the ACSC investigates an incident, staff advise the affected entity of the vulnerabilities they identify and give advice on the necessary remediation and mitigations to put in place. The ACSC then uses this information to update general cyber security advice provided to other Commonwealth entities, as well as industry and the public, to help successfully mitigate vulnerabilities. For example, the use of malicious Microsoft Office macros was observed through the ACSC's incident response function. As a result, the ACSC updated its advice and disseminated it to other entities to ensure they could put the necessary protections in place.

In 2019, the ACSC responded to 427 incidents affecting Commonwealth entities – 65 percent of which were self-reported to the ACSC. The remaining 35 percent were identified through: ACSC investigations; reporting from international partners and third parties; and analysis of a variety of classified and open-source material. The breakdown of incidents and type, as recorded by the ACSC in 2019, is reflected in Figure 1.

Commonwealth entity cyber security incidents

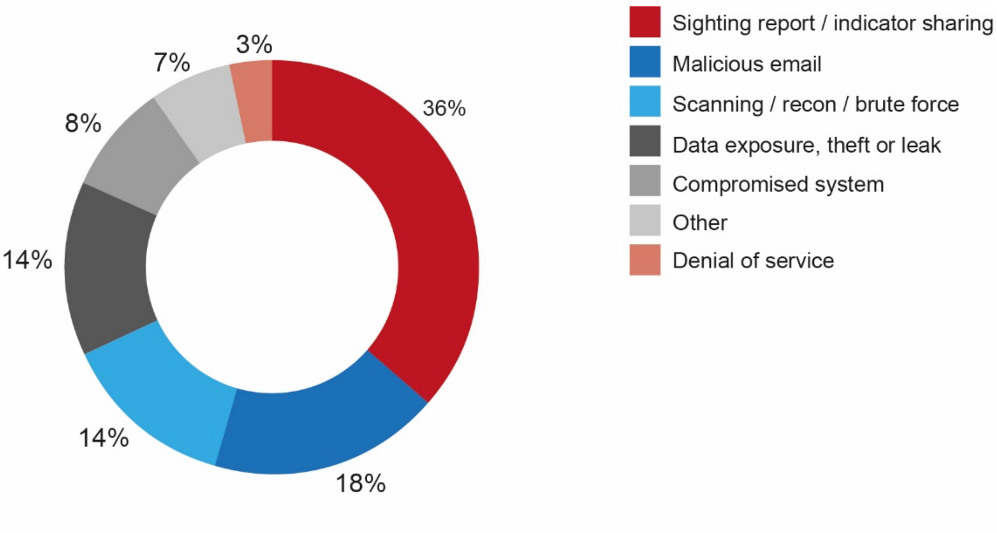

Figure 1: Commonwealth entity cyber security incidents reported to the ACSC in 2019

- *Sighting report/indicator sharing: Reporting of suspected and confirmed indicators of compromise (for example, IP addresses and domain names).*
- *Malicious email: An email sent with the malicious intent to gain unauthorised access to a network, account, database or website.*
- *Scanning, reconnaissance (recon), brute force: Unauthorised scanning of network ports and systematic attempts to guess passwords through repeated attempts.*
- *Data exposure, theft or leak: Unauthorised access, use or disclosure of official information.*
- *Compromised system: A system on which an actor has accessed or modified a network, account, database or website without authorisation.*
- *Denial of Service: Deliberate or accidental action of overloading, interrupting or shutting down of services temporarily or permanently, preventing legitimate users from accessing a service.*
- *Other: Reports that do not meet any of the above malicious cyber-specific criteria (for example, domain squatting and domain spoofing).*

Some of the cyber incidents involving Commonwealth entities were high-profile and complex, including the malicious activity affecting the network of the Department of Parliamentary Services. The Government's cyber experts assess that a sophisticated actor was responsible for this malicious activity. However, the activity was detected by security and intelligence agencies who rapidly responded, mitigating the threat and remediating the affected systems.

The Commonwealth's cyber security posture

Levels of cyber security maturity vary across the Australian Government. While the cyber security posture of Commonwealth entities continues to improve, entities remain vulnerable to cyber threats. Additional work is required for Commonwealth entities to reach a mature and resilient cyber security posture that meets the evolving threat environment.

Essential Eight implementation is improving.

The ACSC recommends all Commonwealth entities implement the *Essential Eight* as a baseline. In 2019, implementation of the *Essential Eight* across Commonwealth entities improved slightly in comparison to previous years. More entities are taking steps to apply the baseline strategies and increase the maturity of their implementation. Entities are concurrently assessing their risk environment and implementing further recommended controls drawn from the *Strategies to Mitigate Cyber Security Incidents*.

Some entities excel, integrating the ACSC *Strategies to Mitigate Cyber Security Incidents* guidance into their cyber security practices, with sophisticated and highly effective security controls in place to mitigate cyber threats. Although other entities are still working to implement the baseline controls, with the support of the ACSC they are actively taking important steps to maintain and further strengthen their cyber security posture.

Particular improvements noted through the *ACSC Cyber Security Survey* between 2018 and 2019 include:

- 50 percent more Commonwealth entities have progressed from partly to mostly aligned with the *Essential Eight* strategy on user application hardening. This helps reduce the potential attack surface of Commonwealth workstations, as well as limiting adversaries' ability to bypass other security controls.
- 35 percent more Commonwealth entities have progressed from partly to mostly aligned with the *Essential Eight* strategy on multi-factor authentication. This improvement makes it more difficult for an adversary to steal legitimate credentials to enable malicious activities on a network or internet-facing services.
- 33 percent more Commonwealth entities have progressed from partly to mostly aligned with the *Essential Eight* strategy on configuring Microsoft Office macros. This will reduce the ability of malicious actors to use macros as a vector to compromise workstations.

However, the baseline adoption of the Essential Eight across the Australian Government still requires further improvement to meet the rapidly evolving cyber security threat environment.

The *ACSC Cyber Security Survey* found current implementation of the *Essential Eight* must improve to meet the rapid changes taking place in the broader cyber security threat landscape. This finding was supported by AGD's analysis of entities' PSPF maturity reporting in 2018–19, which indicated that cyber security remains an important priority for agencies, with significant work to be done to raise the maturity of their mitigations of common and emerging cyber threats.

While all of the Commonwealth entities assessed through the Cyber Uplift sprints were found to be taking positive and proactive steps to improve their cyber security, the ACSC assessed that they had not yet achieved the recommended maturity level for the *Essential Eight*. As a result, these entities are vulnerable to current cyber threats targeting the Australian Government.

The following key findings highlight the issues which were impacting the ability of some entities to achieve a more mature and resilient security posture:

- Entities had inadequate visibility of their information systems and data holdings.
- Entities had a number of obsolete and unsupported operating systems and applications.
- Many entities would benefit from a faster ICT modernisation cycle, noting the *Essential Eight* is significantly easier to implement on modern ICT systems (this would allow them to immediately benefit from modern security features, and then more efficiently apply best practice cyber security).
- Entities misunderstood, misinterpreted and inconsistently applied the *Essential Eight*.
- Entities had ineffective risk management practices.

Implementation of the mandatory Top Four Strategies to Mitigate Cyber Security Incidents is incomplete.

As part of *Policy 10: Safeguarding information from cyber threats*, the PSPF mandates that all non-corporate Commonwealth entities implement the *Top Four Strategies to Mitigate Cyber Security Incidents*[6]. Initial analysis from AGD's 2018-19 PSPF maturity reporting shows that entities' self-assessed implementation of the *Top Four* remains at low levels across the Australian Government, with:

- 73 per cent of non-corporate Commonwealth entities reporting *ad hoc*[7] or *developing*[8] levels of maturity (see Figure 2)
- 67 per cent of non-corporate Commonwealth entities acknowledging the need to raise the maturity of their cyber security against at least one of the *Top Four* strategies.

[6] ASD's *Essential Eight* incorporates the *Top Four* mitigation strategies (application whitelisting, patching applications, restricting administrative privileges, and patching operating systems) as mandated by the PSPF's *Policy 10: Safeguarding information from cyber threats.*

[7] The *ad hoc* maturity rating is defined as partial or basic implementation and management of PSPF core and supporting requirements.

[8] The *developing* maturity rating is defined as substantial, but not fully effective, implementation and management of PSPF core and supporting requirements.

2018-19 PSPF maturity reporting

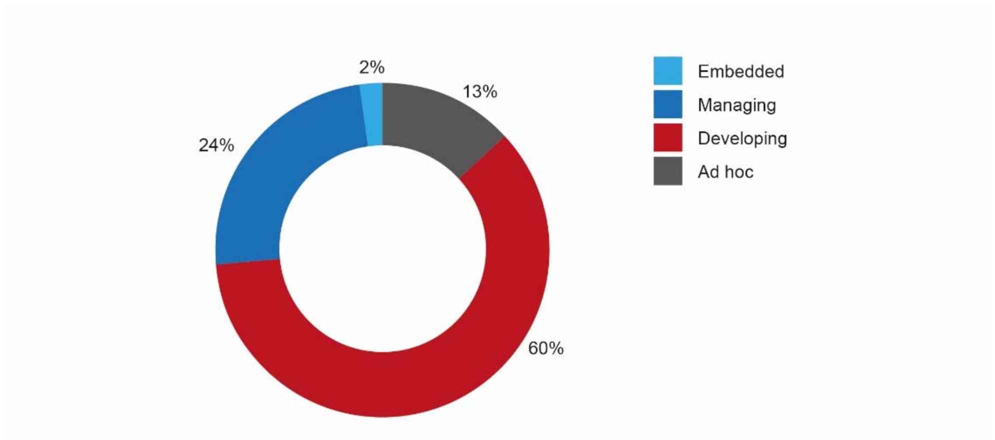

Figure 2: 2018-19 PSPF maturity reporting by non-corporate Commonwealth entities – self-assessment responses to PSPF Policy 10 Safeguarding information from cyber threats.

The Cyber Uplift program has improved entities' cyber security posture.

Through the Cyber Uplift, the ACSC provided advice and assistance to entities. This has already resulted in a noticeable change in entities' cyber security posture, including:

- increasing the visibility and understanding of the systems, data holdings and networks of entities – both for the ACSC and the entity itself – which allows faster identification of risks and vulnerabilities and prioritisation of security improvements
- increasing engagement and information sharing between the ACSC and Commonwealth entities, as well as between entities
- removing obsolete and unsupported operating systems and applications, or, where these systems and applications remain necessary, developing and incorporating protective measures
- rectifying weaknesses in application whitelisting to better prevent the potential execution of malicious software in information systems
- increasing staff knowledge of cyber security and promoting the importance of everyday cyber hygiene practices to protect entities
- increasing the maturity level of Microsoft Office macro settings, daily backups and user application hardening.

While additional work is required in order for all Commonwealth entities to achieve, and maintain, the recommended baseline level of cyber security maturity, the impact of the increasing implementation of the *Essential Eight* – along with other mitigation strategies – is improving the Commonwealth's cyber security posture.

Commonwealth entities are improving their internal cyber security culture.

While financial and staffing issues are the most commonly reported obstacles to implementing various elements of the *Essential Eight*, Commonwealth entities are still making positive progress in improving their cyber security culture. It is critical that good cyber security practices are part of core business. Data from 2019 demonstrated that many entities have improved their documenting of cyber incident management plans, procedures and risk assessments – and senior management have appropriate oversight and involvement. There are a number of entities demonstrating other indicators of a good cyber security posture, including: cyber security training for employees (see Case Study 3); vulnerability scanning capabilities; more mature controls across their systems; and enterprise-grade password managers for securing passwords.

Despite the increased threats, greater attention to bolster cyber security practices across Commonwealth entities has improved the Australian Government's cyber security posture.

Case Study 3

Even before the Cyber Uplift, many entities were taking proactive steps to improve their cyber security posture. For example, several entities had implemented automatic and continuous phishing awareness training. This included sending regular phishing emails to staff. Staff who clicked on the links were automatically registered for a remedial cyber security training program. Managers were then automatically alerted if their staff did not complete the remedial training in a required timeframe. Importantly, these programs are continually being updated to make staff aware of new tactics being employed by malicious cyber actors.

Implementation of malicious email mitigation strategies has improved across the Commonwealth.

Socially engineered emails containing malicious attachments and embedded links are routinely used in targeted cyber intrusions against organisations. In 2019, the ACSC's CHIPs focused one of its campaigns on combatting fake emails. The ACSC advises that entities can reduce the likelihood of their domains being used to support fake emails by implementing Sender Policy Framework (SPF) and Domain-based Message Authentication, Reporting and Conformance (DMARC) records in their Domain Name System (DNS) configuration[9]. The CHIPs campaign increased the number of Australian Government (.gov.au) domains implementing these strongly recommended fake email mitigation strategies by approximately one third (see Figures 3 and 4).

[9] Additional information on combatting fake emails can be found at https://www.cyber.gov.au/publications/how-to-combat-fake-emails.

Sender Policy Framework (SPF) Implementation

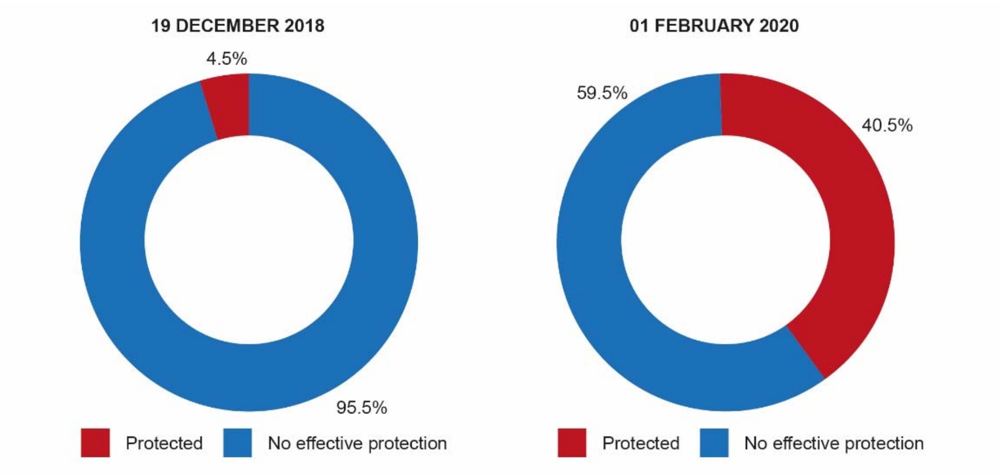

Figure 3: Commonwealth entity implementation of SPF before and after the CHIPs combatting fake emails campaign.

Domain-based Message Authentication, Reporting and Conformance (DMARC) Implementation

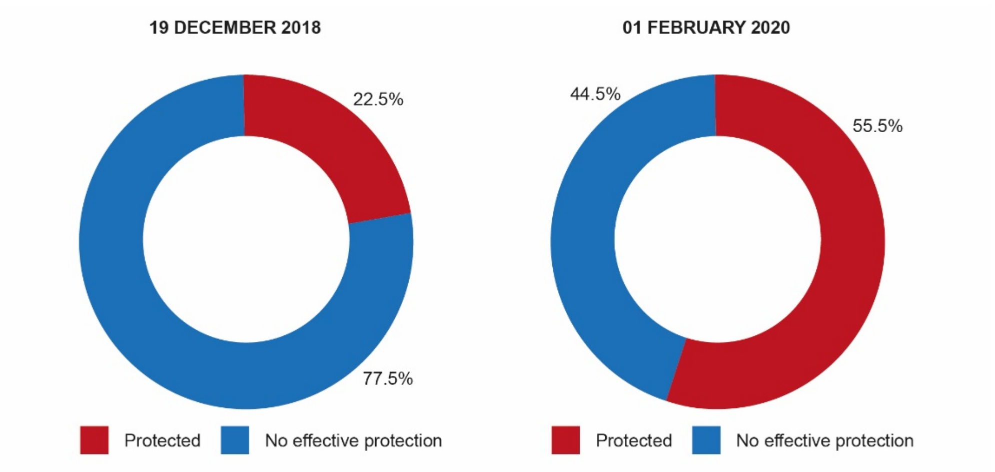

Figure 4: Commonwealth entity implementation of DMARC before and after the CHIPs combatting fake emails campaign.

Commonwealth entities are increasing their capability to identify cyber security events and incidents.

In 2018, most respondents to the *ACSC Cyber Security Survey* were unable to provide data on cyber security events or incidents observed in their entity's environment. In 2019, the majority of respondents reported experiencing hundreds of cyber security events or incidents per day, with only 10 percent unable to provide data (see Figure 5).

Visibility of cyber security events/incidents 2018–19

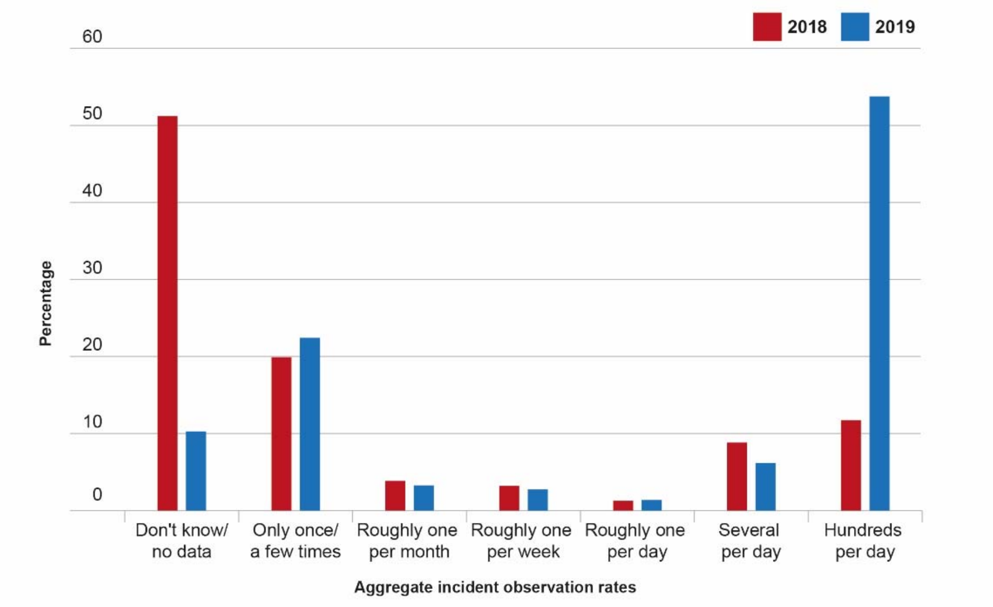

Figure 5: Visibility of cyber security events/incidents 2018–19 – ACSC Cyber Security Survey results.

Next Steps

Commonwealth entities continue to improve their cyber security; however, ongoing effort is required to maintain the currency and effectiveness of cyber security measures. The ACSC continues to help entities improve their cyber security posture and resilience – including by implementing the *Essential Eight*, tailored to the risk level faced – and continues to help entities maintain their cyber security once they reach the right posture.

In 2020, additional areas of effort will include:

- continuing to review the ACSC's cyber security advice, ensuring it is applicable, practical and effective for Commonwealth entities
- ensuring the recommended cyber security measures keep pace with new and emerging technologies and constantly evolving cyber threats
- driving the modernisation of the Australian Government's ICT systems to support the necessary cyber security posture, including stimulating and diversifying the ICT-skills pipeline
- ensuring that baseline cyber security recommendations include detection and response readiness measures appropriate to the current cyber threat environment
- providing security reports, tools and supporting infrastructure to Commonwealth entities to supplement their detection capabilities and improve resilience against cyber threats
- increasing the situational awareness of the scope and scale of malicious activity impacting Australia, including increased monitoring, technical security controls and identifying known vulnerabilities of the networks of Commonwealth entities.