Australian Government
Australian Taxation Office

Australian Taxation Office Submission

Cybersecurity Compliance – Inquiry into Auditor General's report 42 (2016-17)

27 April 2017

Contents

Introduction

1. The Australian Taxation Office (ATO) places high priority on cybersecurity and recognises that confidence in security and safety of data and systems is paramount to offering services to the Australian community. These commitments to cybersecurity are in our Corporate Plan and supported at the ATO Executive level.

2. The ATO continues to enhance our systems to provide better services for the Australian community. We are focused on maintaining the security and integrity of our data and information by understanding threats and protecting our systems from malicious cyber threats as well as preparing incident response plans.

3. Providing the Australian community with more convenient and accessible services requires taking advantage of new and emerging technologies. These new technologies are often accompanied with new and emerging cyber risks. We actively consider and manage these risks so that we continue to meet community expectations by anticipating and responding to cyber threats.

Recommendations and ATO actions

4. Whilst the Audit noted there has been improvement in the overall maturity of the cybersecurity posture of the ATO since 2014, the review also highlighted further improvements to strengthen cybersecurity.

5. The ATO has given significant priority to cybersecurity, agreed with recommendations of the Audit, and has put in place a number of actions to implement these recommendations to strengthen governance arrangements and the overall level of compliance with the Australian Signal's Directorate Top Four Mitigation Strategies.

Recommendation 1

The ANAO recommends that entities periodically assess their cybersecurity activities to provide assurance that the activities are accurately aligned with the outcomes of the Top Four mitigation strategies and entities' own ICT security objectives. This applies regardless of whether cybersecurity activities are insourced or outsourced.

6. Actions implemented to address recommendation one to date:

- Appointing an SES Band 2 as the Chief Security Officer who is accountable for taking a multifaceted approach to cybersecurity; including regular information technology risk and threat assessments, strategy and policy (including a revised whitelisting strategy), system certification reviews, and a monitoring and compliance regime.
- Commissioning the development of an overarching security strategy that encompasses all elements of security as well as cybersecurity.
- The ATO Security Committee is monitoring the status of the implementation of the recommendations from ANAO and other audits relating to cybersecurity.
- Creating one integrated Information and IT Security functional unit.
- Strengthening whitelisting and patching policies with external vendors.

7. Future actions planned during 2017 to address recommendation one:

- External advice is scheduled for October 2017 to assess the ATO's cybersecurity activities to provide assurance that the activities are aligned with the outcomes of the Top Four mitigation strategies, the ATO's ICT security objectives and governance arrangements are effective.

Recommendation 2

The ANAO recommends that entities improve their governance arrangements by:

a) Asserting cybersecurity as a priority within the context of their entity-wide strategic objective;

b) Ensuring appropriate executive oversight of cybersecurity;

c) Implementing a collective approach to cybersecurity risk management; and

d) Conducting regular reviews and assessments of their governance arrangements to ensure its effectiveness.

8. Actions implemented to address recommendation two:

- Recommendation 2.a - The importance and priority of cybersecurity is reflected in the ATO's Corporate Plan.
- Recommendation 2.b - The ATO has increased and strengthened executive oversight arrangements of cybersecurity by:
  - The ATO's Security Committee monitoring the ATO's level of compliance with the Top Four mitigation strategies.
  - Reporting on level of compliance with the Top Four is provided to the ATO's Chief Information Officer and the Security Committee on a monthly basis.
  - The ATO's level of compliance with cybersecurity controls will also form part of the regular reporting to the newly formed Risk Management Committee.
- Recommendation 2.b - The ATO has strengthened security governance arrangements with third party suppliers to more closely monitor the status of the ATO's compliance with the Top Four:
  - Full baseline Top Four governance reporting with our third party suppliers to monitor the level of compliance has been established. This reporting will be extended to include the Essential Eight mitigation activities during 2017.
  - Independent validation processes on the information provided to the ATO by third parties have commenced. The ATO is now directly accessing third party supplier whitelisting and patching tools to validate and assure information provided by third party suppliers.
- Recommendation 2.c - The ATO's regular program of systems security certifications and risk assessments, which cover the Top Four as well as the Australian Government Information Security Manual (ISM) controls remain in place and reporting on these has been enhanced to more effectively highlight matters relating to the Top Four.
- Recommendation 2.c - The ATO has established a Security Operations Centre to facilitate real-time monitoring of security threats, to increase the focus on external threats and to actively inform security risks facing the ATO.

9. Future actions planned during 2017 to address recommendation two:

   - Recommendation 2.a - Expansion of all reporting to encompass the Essential Eight mitigation activities.
   - Recommendation 2.c - Transitioning to the new ATO Enterprise Risk Management Framework which facilitates and ensures a collective approach to cybersecurity risk. The ATO is transitioning to the new framework during 2017.
   - Recommendation 2.d - External advice is scheduled for October 2017 which includes reviewing the effectiveness of cyber governance structures.
   - Recommendation 2.d - Strengthening contract clauses to more effectively ensure compliance by third party providers.

Status of compliance with the Australian Signals Directorate Top Four mitigation strategies

10. The ATO increased transparency and overt commitment to compliance with the Top Four, is showing an overall improvement and a pathway to achieve full compliance this year.

11. The ATO takes a risk based approach to cyber compliance which includes considering and managing cybersecurity risk, and balancing this with business delivery and the ATO's commitment to contemporary and accessible services for the community.

12. The current levels of compliance, in particular with patching and whitelisting have been temporarily impacted by the ATO's recent SAN (storage area network) hardware issues. In support of the full restoration and remediation, whitelisting on some servers had to be disabled and is being re-enabled as the restoration progresses. The restoration activities have also had the impact of delaying some patching cycles. Patching cycles have recommenced and the majority of servers will have whitelisting re-enabled by June 2017.

13. An overview of the ATO's status of compliance with the Australian Signals Directorate Top Four as at May 2017 is at Appendix 1.

Other cybersecurity activity undertaken by the ATO

14. The ATO's investment and commitment to cybersecurity is not limited to compliance with the Top Four mitigation strategies and working on the Essential Eight.

15. The ATO have set up a dedicated Security Operations Centre to monitor, detect and respond to cybersecurity threats facing the ATO.

16. Multiple layers of defences are built into our environment to prevent, detect and deter ongoing persistent threats including layered security gateway infrastructure, intrusion detection systems, intrusion prevention systems and data loss prevention tools.

17. Implementation of an end-to-end IT security process has provided assurance that security is embedded into systems from the initial conception stage to deployment into production.

18. The ATO have an established cybersecurity vulnerability management program that undertakes:

    - Penetration testing of systems to detect vulnerabilities before and after implementation. Recommendations on how to manage the risks are made and acted on.
    - Security incident response processes.
    - Intelligence activities to ensure overall 'visibility' of what is occurring within the ATO network in near-real time. This is done through the collection and analysis of a range of data.

19. Other activities and capabilities to strengthen cyber resilience include:

    - Distributed Denial of Service Attack protection.
    - Shadow IT monitoring and detection.
    - Data Loss Prevention.
    - Security architecture reviews.
    - Audit Logging framework and centralised logging store.
    - Centralised access control framework and monitoring.
    - IT security risk assessment, management and treatment.
    - Static and dynamic code reviews.
    - Compliance reviews and iRAP audits (certification/accreditation reviews).
    - External security assessment and assurance reviews.
    - ATO covert operatives.
    - Support for the public to verify or report a scam using the ATO name.

Appendix 1

The ATO's status of compliance with the Australian Signals Directorate Top Four mitigation strategies as at May 2017

1. Application Whitelisting

Overall Status: Watch Item

SERVERS	Number of Critical Servers	Compliance Rate	May 2017	Nov 2016
Midrange Servers (including hosted enterprise applications)	2559	57% (Windows) 6% (Linux)		
Managed Network Services (including telephony, call centres etc.)	27	67%		
End-User Computing	185	100%		
DESKTOPS	**Number of Desktops**	**Compliance Rate**	**May 2017**	**Nov 2016**
Desktops	28,325	100%		

20. Whilst the ATO was fully compliant in November 2016 with whitelisting our Windows based servers, our current levels of compliance have been impacted by the ATO's recent SAN outages. In support of the full restoration and remediation program, whitelisting on a range of servers needed to be disabled and re-enabled as the restoration progresses. We have plans in place to progressively re-enable whitelisting in coming months taking into account tax time activities.

2. Patch Applications

Overall Status: On Track

High Risk Applications	Compliance Rate	May 2017	Nov 2016
Adobe Reader	99.1%		
Java	99.4%		
Flash Player Active X	99.8%		
Flash Player Plugin	99.8%		
Firefox	100%		Not Assessed

21. The ATO has a patching policy in place and a regular patching cycle to ensure patches are deployed on a cyclical basis. All critical patches are deployed within 48 hours.

3. Patching Operating Systems

Overall Status : Watch Item

PATCH CYCLE - SERVERS	Number to be patched (production & critical)	May 2017	Nov 2016
Midrange Servers (including hosted enterprise applications)	2697	Windows Linux	
Managed Network Services (including telephony, call centres etc)	27		
End-User Computing	485		
PATCH CYCLE - DESKTOP	**Number of Desktops**	**May 2017**	**Nov 2016**
Desktops	23,309		

22. The ATO's overall level of compliance with our patching policy and cycle has improved overall since November 2016.

23. Our plans to achieve full compliance have been impacted by the ATO's recent SAN outages. In support of the full restoration and remediation program, some patching cycles have been delayed. Patching has resumed and the remaining patching in the Linux environment is scheduled for quarter two, after critical Tax Time activities.

4. Restrict Administrative Privileges

Overall Status: On Track

Unique Number of Privileged Accounts	May 2017	Nov 2016
851		

System accesses, in particular privileged access, is monitored and regularly reviewed.