Submission

The Joint Committee of Public Accounts and Audit

CYBERSECURITY COMPLIANCE - INQUIRY INTO AUDITOR-GENERAL'S REPORT 42 (2016-17)

Contact details:

Ian Brightwell
[redacted]

Ian Brightwell: [redacted].....

Date: 30 October 2016

The Joint Committee of Public Accounts and Audit

CYBERSECURITY COMPLIANCE - INQUIRY INTO AUDITOR-GENERAL'S REPORT 42 (2016-17)

Table of Contents

Author: Ian Brightwell

Recommendations

The author commends the following recommendations for the Committee's consideration.

***Recommendation 1**: Remove whitelisting from the mandatory list of strategies and focus on implementing a full set of ICT general controls to a level appropriate to the agency risk assessment.*

***Recommendation 2**: The parliament should consider issuing terms of reference for an inquiry into the cause of the recent ATO failures and reasons why the ICT general controls around business continuity did not appear to recover the systems in a satisfactory period of time.*

***Recommendation 3**: Make mandatory those controls that improve agencies ability to implement good network and system management practices and the continuous independent monitoring of these practices.*

***Recommendation 4**: Make mandatory those controls that improve detection of potential malicious network activity by continuous monitoring of network and user activity.*

***Recommendation 5**: Make mandatory controls that ensure the capture of adequate immutable log information to assist the assessment of breaches when they occur.*

***Recommendation 6**: The committee should consider recommending ANAO and agencies conduct future cyber resilience assessments using a broadly-based assessment approach rather than assessing against a narrow set of four mandatory controls.*

***Recommendation 7**: The committee should consider recommending ASD develop documentation to allow agencies to readily assess their security posture using CRR/RMM and related control document rather than directly against ISM when conducting future cyber resilience self-assessments.*

***Recommendation 8**: The committee should consider recommending to government that the Chief Information Security Officer (CISO) position not be a combined with a position within the technology delivery area and have a direct reporting line to the CEO.*

1 Introduction

The author would like to commend the parliament for undertaking this inquiry and the ANAO for their excellent work in shining a light on the state of cyber resilience in federal government agencies.

The findings of this and earlier audit reports would be of no surprise to many who have worked in agencies at senior levels and understand the challenges of allocating resources to these tasks and the resistance faced by and from other executives whose focus is on "real" business issues.

The slow rate of cyber resilience improvement in many agencies can be attributed to a range of factors including: the requirement to implement difficult controls such as whitelisting, lack of management support to prioritise cyber security and limited funding plus dealing with the inevitable tensions between the drive for digital transformation verse maintaining an environment which is secure.

Given the increasingly threat environment in which agencies operate and the slow progress in implementation of mitigation strategies it would be difficult to believe that the commonwealth's information is better protected now than it was in 2014. Commonwealth agencies need to implement and be audited on a defence in depth strategy which not only tries to protect systems against targeted and opportunistic attacks but also detects when intrusions have occurred from both targeted and non-targeted attacks.

The detection of intrusions is as potentially more important than their prevention. A recent report by Fireye[1] identified the average breach dwell time (days from breach to detection) in APAC is 172 days which is worse than the rest of the world, but a vast improvement on the previous year's result where it was over 500 days for APAC. When this information is coupled with the fact Fireye's "Red Team"[2] typically obtains access to domain administrator credentials within three days of the initial breach, which means a competent attacker would have full control of a network for 169 days before detection. It is also interesting to note that nearly a half of breached organisations had to be told by external parties they were breached rather than detecting the breach themselves.

2 Author Background

The author[3] of this submission has worked as an ICT executive and consultant with for over 30 years. He is certified in in the Governance of Enterprise IT (CGEIT)[4] by ISACA and is an active member of the Australian Information Security Association. He has been responsible for managing complex government systems and has been the Senior Responsible Officer for Information Security in a high security profile government agency. He is currently a government gateway reviewer of ICT programs and an executive advocate for improving cyber resilience in organisations.

[1] Fireye M-Trends 2017: Trends from the year's breaches and cyber attacks
https://www.fireeye.com/current-threats/annual-threat-report.html
[2] Attackers sanctioned by the client to test a company's system posture covertly.
[3] Ian Brightwell – Linkedin Profile
https://www.linkedin.com/in/ian-brightwell-a038573/
[4] ISACA Certification in the Governance of Enterprise IT (CGEIT)
http://www.isaca.org/Certification/CGEIT-Certified-in-the-Governance-of-Enterprise-IT/Pages/default.aspx

3 Policy Environment

The ANAO[5] report mainly measured cyber resilience by assessing agency compliance against the (minimum) mandatory requirements of the Australian Governments Protective Security Policy Framework (PSPF). This involved assessing agencies against the "Top 4"[6] mandatory "Strategies to Mitigate Targeted Cyber Intrusions" as detailed in the Australian Government Information Security Manual[7] (ISM).

PSPF mandatory requirements within INFOSEC 4 requires agencies to implement the "Top 4" Strategies. The implementation of the remaining 31 Strategies is also strongly recommended; however, agencies can prioritise these depending on business requirements and the risk profile of each system.

The "Top 4" Strategies are:

1. application whitelisting
2. patch applications
3. patch operating systems
4. restrict administrative privileges.

In early 2017 the "Top 4" mandatory strategies was expanded to 8 strategies. They are now called "Strategies to Mitigate Cyber Security Incidents" dropping the reference to targeted. The Australian Signals Directorate (ASD) deem that they replace Strategies to Mitigate Targeted Cyber Intrusions as of February 2017[8], although it is not clear to the author if PSPF requires agencies to comply with the new 8 or just the old 4 strategies. Regardless, of whether 4 or 8 strategies are mandatory, one thing the above changes show is that any concept of a list of minimum mandatory strategies is a moving target. This means that agencies which may be compliant now will not be compliant in the near future just because the goal posts will have moved.

The ANAO's reports have highlighted that some of the audited agencies are not compliant with many of the current mandatory strategies let alone the additional 4 essential strategies. Also, the agencies progress to compliance with the current 4 strategies is slow. ANAO found even after three years there were still shortfalls in the implementation of the "Top 4" strategies. The report also identified that two agencies believed they were compliant with strategies but ANAO did not agree, which raises doubts about the viability of self-assessment.

Recommendation 2 of the ANAO report suggested entities should improve their governance arrangements, by asserting cybersecurity as a priority within the context of their entity-wide strategic objective; ensuring appropriate executive oversight of cybersecurity; implementing a collective approach to cybersecurity risk management; and conducting regular reviews and assessments of their governance arrangements to ensure its effectiveness. The author fully supports these recommendations and believes that the regular reviews and assessments should be expanded

[5] Australian National Audit Office
[6] Top 4 Strategies to Mitigate Targeted Cyber Intrusions: Mandatory Requirement Explained
https://www.asd.gov.au/infosec/top-mitigations/top-4-strategies-explained.htm
[7] Australian Government Information Security Manual (ISM) from Australian Signals Directorate (ASD)
https://www.asd.gov.au/infosec/ism/
[8] Strategies to Mitigate Cyber Security Incidents
https://www.asd.gov.au/infosec/mitigationstrategies.htm

to require agencies to conduct broad based resilience assessments using both internal reviewers and independent external reviewers to ensure the integrity of the process.

The ANAO report focused on the measurement of agency implementation of the “Top 4” strategies and two ICT General controls as an indicator of agency cyber resilience. The implementation of this limited set of strategies does not in the authors view give a good indication of an agencies security posture and cyber resilience. The Committee needs to consider whether the ANAO’s current reporting approach is an effective indication of cyber resilience or whether a broader assessment of cyber resilience by using a full set if IT general controls would be a more effective indicator of resilience.

The ANAO report focused on the measurement of agency implementation of the “Top 4” strategies and two ICT General controls as an indicator of agency cyber resilience. The implementation of this limited set of strategies does not in the authors view give a good indication of an agencies security posture and cyber resilience. The Committee needs to consider whether the ANAO’s current reporting approach is an effective indication of cyber resilience or whether a broader assessment of cyber resilience by using a full set if IT general controls would be a more effective indicator of resilience.

4 Is Whitelisting worth the Effort?

It is indisputable that the “Top 4” strategies (which have whitelisting as the top strategy) if implemented fully would reduce the likelihood of an agency either getting breached or the extent of a breach. However, this does not mean these are the best strategies for every agency to implement. The question that needs to be asked is “Are these the right mandatory strategies for agencies at this point in time?” or conversely “Are there more effective mandatory strategies to implement or even should we have mandatory strategies?”.

The report also stated that to become cyber resilient, an entity must first establish a sound ICT general controls framework. ICT general controls provide a stable and reliable foundation upon which other processes and controls can be built. It is the authors view that it is inappropriate for agencies to try and implement the “Top 4” mitigation strategies without effective controls in place. A finding of the report was that the of the three entities audited, only the Department of Human Services was cyber resilient, the Australian Taxation Office and the Department of Immigration and Border Protection need to improve their governance arrangements and prioritise cybersecurity. In general this means they must improve their ICT general controls.

The author shares the auditors view that many entities do not have sound ICT general controls framework in place. The report further says this framework provides an entity with a stable and reliable ICT environment and forms the foundation upon which other processes and controls can be built. ICT general controls include controls over: ICT governance; ICT infrastructure; acquiring and developing applications; logical user access to ICT infrastructure, applications and data; and making changes to ICT systems and applications. Agencies can only assess if they have these controls in place by using a broad-based resilience assessment approach.

It should also be noted the ANAO report only appears to have looked at two elements of the ICT general controls framework—logical access control and change management. It is not clear from the report what the state of other ICT general controls are within each agency.

The current top mandatory strategy is to implement a very aggressive form of whitelisting. Application whitelisting protects ICT systems against unauthorised applications running on them. Its purpose is to protect systems and networks from harmful applications. The Information Security Manual (ISM) requires entities to implement application whitelisting for both desktops and servers. Below are the actual whitelisting controls as taken from the 2016 Australian Government Information Security Manual CONTROLS[9].

> **Control: 0843**; Agencies must use an application whitelisting solution within Standard Operating Environments (SOE)s to restrict the execution of programs and DLL s to an approved set.
>
> **Control: 0846**; Users and system administrators must not be allowed to temporarily or permanently disable, bypass or be exempt from application whitelisting mechanisms.
>
> **Control: 0955**; Agencies must implement application whitelisting using at least one of the methods:
>
> - cryptographic hashes
> - publisher certificates
> - absolute paths
> - parent folders.
>
> **Control: 1391**; When implementing application whitelisting using parent folder rules, file system permissions must be configured to prevent users and system administrators from adding or modifying files in authorised parent folders.
>
> **Control: 1392**; When implementing application whitelisting using absolute path rules, file system permissions must be configured to prevent users and system administrators from modifying files that are permitted to run.

The report clearly showed that even after 3 years whitelisting had not been implemented across all agencies. Both the ATO and Immigration had not effectively implemented application whitelisting on their servers. Only Immigration had not effectively implemented application whitelisting on its desktops. This contravenes the Information Security Manual and the entities' own ICT security policies and begs the question why has this not been done?

The implementation of the above whitelisting controls across every device in a typical agency would in my view be impossible and potentially counterproductive. I say counterproductive because a partial implementation could cause more disruption than benefit and take valuable resources away from implementing more appropriate ICT general controls which would be more beneficial for improving agency cyber security posture. Whitelisting is most easily implemented in agencies which have a very standardised computer environment that utilises limited number of Standard Operating Environments (SOE)s which do not change regularly. This is at odds with the needs of typical agencies have groups of users who need a flexible environment that is incompatible with whitelisting.

[9] 2016 Australian Government Information Security Manual CONTROLS
https://www.asd.gov.au/publications/Information_Security_Manual_2016_Controls.pdf

The following has been extracted from NIST Special Publication 800-167, Guide to Application Whitelisting[10] and clearly identifies implementation it in a general-purpose agency network environment may not be suitable.

> *Application whitelisting solutions are **generally strongly recommended for hosts in high-risk environments where security outweighs unrestricted functionality**. Suitability for typical managed environments depends on how tightly the hosts are managed and the extent of the risks that they face. **Organizations considering application whitelisting deployment in a typical managed environment should perform a risk assessment to determine whether the security benefits provided by application whitelisting outweigh its possible negative impact on operations.** Organizations should also be mindful **that they will need dedicated staff managing and maintaining the application whitelisting solution** depending on the scale and specifics of the solution implemented, similar to handling an enterprise antivirus or intrusion detection solution.*

My own view is that whitelisting is a useful control for only some networks and only deals with individual computers running Linux and Windows, which means all other devices on networks like printers, routers, scanners, cameras are not covered. Additionally, most agencies are not sufficiently mature to implement whitelisting on their general networks and cannot make the investment to understand and specify what software their people have to use and determine if it is safe. Therefore, the effort required to implement and maintain blocking whitelisting as defined above across every device in a typical agency is a questionable use of resources when other properly implemented ICT general controls strategies would yield greater benefits for the resource usage.

> ***Recommendation 1**: Remove whitelisting from the mandatory list of strategies and focus on implementing a full set of ICT general controls to a level appropriate to the agency risk assessment.*

5 What Controls should be Implemented?

Recent studies have shown that many of the cyber breaches are opportunistic and rely on gross misconfigurations of systems, even the more targeted attacks often rely on misconfigurations. A report[11] from Secureworks identified that 88% of attacks are opportunistic as opposed to 12% being targeted. This supports a view I share with the SecureWorks Director of the Counter Threat Unit (CTU) Cyber Intelligence Cell; that the "Basic health and hygiene across the IT estate is still something that most organisations fail at". Also, the Director of SecureWorks' Incident Response and Digital Forensics practice said, "Most organisations should stop worrying about zero-day attacks, when there are so many other threats that are much more prevalent. The obvious conclusion RETURN TO THE BASICS to Strengthen Your Security Posture.

[10] NIST Special Publication 800-167, Guide to Application Whitelisting
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf
[11] 2017 Cybersecurity Threat Insights Report for Leaders, Secureworks, February 2017.
https://www.secureworks.com/resources/rp-cybersecurity-threat-insights-2017
https://1drv.ms/b/s!Akm0GxLL0Nuo0En3zgKlV3fg5HK5

An indication of the need for agencies to improve their basic ICT general controls is shown by the problems currently experienced by the ATO[12]. I recently wrote about these problems[13] and expressed a view that the apparent inability of the ATO to recover from their HPE SAN failure was an indication that their business continuity planning had failed. I was not concerned that they had a technical problem with their SAN my concern was that even after several months of trying they still had not fully recovered and appeared not to have a stable environment. If they had implemented their ICT general controls fully they would have had an ability to recover from backup within an acceptable timeframe. It appears they had either not tested this capability or had not implemented it which is a general control failure. I will very be interested to read the PWC report[14] on this matter which should be made public.

> ***Recommendation 2****: The parliament should consider issuing terms of reference for an inquiry into the cause of the recent ATO failures and reasons why the ICT general controls around business continuity did not appear to recover the systems in a satisfactory period of time.*

The 4 mandatory strategies defined through PSPF in ISM INFOSEC 4 are largely focused on preventing targeted cyber breaches not dealing with the basics of network management. Basics would include agencies knowing what information, devices and users make-up their network and can they detect if a device is misconfigured or a user is operating outside normal parameters.

There is a strong argument for the mandatory requirements to also include detection of misconfigurations rather than focus on prevention of intrusions by use of Whitelisting. Broad based whitelisting is very difficult to implement and intrusive for users and also very expensive to manage. It also does not prevent intrusions which use scripts that drive legitimate system tools. Conversely improved documentation and configuration of systems and networks is simpler to implement and relatively unobtrusive to the rest of the organisation and has the benefit of improving the operational reliability of systems.

> ***Recommendation 3****: Make mandatory those controls that improve agencies ability to implement good network and system management practices and the continuous independent monitoring of these practices.*

It is generally accepted that breaches will occur no matter how well agencies protect their networks, so detection of malicious operational anomalies through the improvement in monitoring practices should be the top mandatory requirement. This means capturing adequate logs and checking them with the right tools and skilled staff should be mandatory. The benefits of a rapid detection of a breach by the monitoring of anomalous network and user activity regularly and having adequate logging in place is in the authors view more important than trying to prevent attacks by implementing full whitelisting of all systems.

> ***Recommendation 4****: Make mandatory those controls that improve detection of potential malicious network activity by continuous monitoring of network and user activity.*

---

[12] ATO systems update
http://lets-talk.ato.gov.au/ato-systems-update
[13] Opinion: Are the ATO and Census failures just the tip of the iceberg?
http://cdn.cio.com.au/article/612649/opinion-ato-census-failures-just-tip-iceberg/
[14] Australian Taxation Office successfully replaces SAN, web site then fails anyway
https://www.theregister.co.uk/2017/04/19/ato_san_upgrade_succeeded/

***Recommendation 5**: Make mandatory controls that ensure the capture of adequate immutable log information to assist the assessment of breaches when they occur.*

6 How to best Assess Cyber Resilience?

It appears the ANAO assesses cyber resilience by assessing agencies implementation of the "Top 4" strategies and two ICT general controls. This approach only takes a very narrow view of what other countries governments believe constitutes cyber resilience. Most overseas resilience assessment methodologies are based on a much broader set of criteria for measuring cyber resilience.

The US government use Cyber Resilience Review (CRR)[15] assessment methodology developed by the US Department of Homeland Security (DHS) and is based on the CERT Resilience Management Model (RMM)[16]. The goal of the appraisal is to develop a broad understanding of an organisation's operational resilience and ability to manage cyber risk to its critical services during normal operations and times of operational stress and crisis.

One of the fundamental principles of the CRR is the idea that an organisation deploys its assets (people, information, technology, and facilities) in support of specific operational missions (i.e., critical services). Applying this principle, the CRR seeks to understand an organisation's capacities and capabilities in performing, planning, managing, measuring, and defining cybersecurity practices and behaviours in the following ten domains:

- **Asset Management** [pdf]: The Asset Management guide focuses on the processes used to identify, document, and manage the organisation s assets.
- **Controls Management** [pdf]: The Controls Management guide focuses on the processes used to define, analyse, assess, and manage the organisation s controls.
- **Configuration and Change Management** [pdf]: The Configuration and Change Management Guide focuses on the processes used to ensure the integrity of an organisation s assets.
- **Vulnerability Management** [pdf]: The Vulnerability Management Guide focuses on the processes used to identify, analyse, and manage vulnerabilities within the organisation s operating environment.
- **Incident Management** [pdf]: The Incident Management Guide focuses on the processes used to identify and analyse events, declare incidents, determine a response and improve an organisation s incident management capability.
- **Service Continuity Management** [pdf]: The Service Continuity Management Guide focuses on processes used to ensure the continuity of an organisation s essential services.
- **Risk Management** [pdf]: The Risk Management Guide focuses on process used to identify, analyse, and manage risks to an organisation s critical services.
- **External Dependencies Management** [pdf]: The External Dependencies Management Guide focuses on processes used to establish an appropriate level of controls to manage the risks that are related to the critical service's dependence on the actions of external entities.

[15] Assessments: Cyber Resilience Review (CRR)
https://www.us-cert.gov/ccubedvp/assessments

[16] The Department of Homeland Security (DHS) partnered with the Computer Emergency Response Team (CERT) Division of Carnegie Mellon University's Software Engineering Institute to create the CRR. The CRR is a derivative of the CERT Resilience Management Model (RMM) (http://cert.org/resilience/rmm.html) tailored to the needs of critical infrastructure owners and operators.

- **Training and Awareness** [pdf]: The Training and Awareness Guide focuses on processes used to develop skills and promote awareness for people with roles that support the critical service.
- **Situational Awareness** [pdf]: The Situational Awareness Guide focuses on processes used to discover and analyse information related to the immediate operational stability of the organisation s critical services and to coordinate such information across the enterprise.

The US-CERT appraisal is done using a tool based on RMM which requires some 297 questions to be answered. This tool will prepare a report that can be reviewed by all levels of the organisation. The tool prepares a report which provides an assessment against not only the RMM domains but also CSF. The advantage of using CSF is that several organisations like US-Cert have developed tools which allow organisations to assess their resilience[17].

Additionally, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)[18] has a free Cyber Security Evaluation Tool (CSET®)[19]. It was developed by cybersecurity experts under the direction of the Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). The tool provides users with a systematic and repeatable approach to assessing the security posture of their cyber systems and networks. It includes both high-level and detailed questions related to all industrial control and IT systems. The tool can be adapted to suit different environments and can be used to collate and consolidate information from a range of organisations.

The UK also uses a broader based approach to assessing cyber resilience. The UK has developed and promotes for the private sector an evaluation program called Cyber Essentials[20]. This program allows organisations to assess how resilient they are and is similar in breadth to CSF.

I recently wrote an article[21] outlining how organisations can self-assess their cyber resilience using an approach based on the Cyber Security Framework[22] (CSF). This framework was developed by the US National Institute of Standards and is the most commonly used framework internationally. This framework is free and can be downloaded and used by any organisation. It also worth noting ASIC is undertaking “health checks” with ASX 100 companies also use an approach based on CSF and NIST concepts to assess the security of these companies[23].

The key point to note is that DHS and UK assessment approaches provide a much broader assessment than that done by ANAO using the “Top 4” and a limited set of ICT general controls. The

[17] US-CERT, Assessments: Cyber Resilience Review (CRR)
https://www.us-cert.gov/ccubedvp/assessments
[18] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
https://ics-cert.us-cert.gov/
[19] Cyber Security Evaluation Tool (CSET®)
https://ics-cert.us-cert.gov/Assessments
[20] Cyber Essentials
https://www.cyberaware.gov.uk/cyberessentials/
[21] How to assess your organisation’s cyber security resilience
http://www.cio.com.au/article/612456/how-assess-your-organisation-cyber-security-resilience/
[22] Cyber Security Framework, National Institute of Standards and Technology (NIST)
https://www.nist.gov/cyberframework
[23] Cyber resilience health check
http://asic.gov.au/regulatory-resources/corporate-governance/corporate-governance-articles/cyber-resilience-health-check/

committee needs to recommend ANAO conduct future resilience audits using a broader cyber resilience assessment approach for future audits.

> ***Recommendation 6****: The committee should consider recommending ANAO and agencies conduct future cyber resilience assessments using a broadly-based assessment approach rather than assessing against a narrow set of four mandatory controls.*

Also, the committee needs to consider whether ASD should develop and publicly promote a cross-walk document which maps the relationship between the Australian Government Information Security Manual (ISM) and the more commonly used NIST CSF and Security Controls and CRR/RMM Assessment Procedures for Federal Information Systems and Organizations[24]. If this is done then, agencies can self-assess using more readily available assessment tools which will have broader community support than those only suitable for ISM. Additionally, this approach will assist in the development of a deeper resource pool of people who can conduct assessments for both the public and private sector.

> ***Recommendation 7****: The committee should consider recommending ASD develop documentation to allow agencies to readily assess their security posture using CRR/RMM and related control document rather than directly against ISM when conducting future cyber resilience self-assessments.*

7 Technology Governance

Current practice in agencies is to place the information security role under ICT Management typically two levels down the organisation structure without a direct reporting line to the CEO.

Even the Australian Bureau of Statistics (ABS) after its recent problems do not appear to have fully understood the need for improved cyber governance. They have advertised the replacement position for their new Chief Information Security Officer (CISO) to still be combined with their Chief Information Officer (CIO)[25] role. They also continued to have the position too far down the organisation structure which sends all the wrong signals when considering the significance of technology in their operations.

Note the CISO role is not a technology role and my suggestion for smaller agencies that can't resource a separate CISO is that the Chief Operating Officer (COO) or Chief Risk Officer (CRO) take on the joint role rather than combine with the CIO.

> ***Recommendation 8****: The committee should consider recommending to government that the Chief Information Security Officer (CISO) position not be a combined with a position within the technology delivery area and have a direct reporting line to the CEO.*

[24] NIST Special Publication 800-53 (Rev. 4)
https://nvd.nist.gov/800-53/Rev4/
[25] Opinion: Has the ABS learnt anything from its e-Census DDoS debacle?
http://www.cio.com.au/article/614212/opinion-has-abs-learnt-anything-from-its-e-census-ddos-debacle/