McAfee LLC
Level 20, 201 Miller Street
North Sydney NSW 2060
Australia

3 May 2017

Committee Secretary
Joint Committee of Public Accounts and Audit
PO Box 6021
Parliament House
Canberra ACT 2600

Submission to the Joint Public Accounts and Audit Committee inquiry into Cybersecurity Compliance – Inquiry based on Auditor-General's report 42 (2016-17)

McAfee welcomes the opportunity to make this submission in response to the Joint Public Accounts and Audit Committee inquiry into *Cybersecurity Compliance – Inquiry based on Auditor-General's report 42 (2016-17)*.

In this submission we have addressed the terms of reference put forward by the Joint Committee, that is any items, matters or circumstances connected with the *Auditor General's report 42 (2016-2017)* into how to build cyber resilience in government departments specifically as it relates to implementing the Australian Signals Directorate Top Four Mitigation Strategies, and other strategies, such as the Essential Eight Mitigation Strategies.

We concur with ASD's stated belief that '(i)mplementing the … mitigation strategies can save organisations considerable time, money, effort and reputational damage compared to cleaning up after a compromise.'[1]

Further, as ASD suggests, we are also of the opinion that these are baseline strategies which make it much harder for adversaries – external and internal – to compromise valuable government systems and the data they hold. As we outline in this submission, building true cyber resilience requires a holistic approach which goes beyond simply complying with these guidelines and requires organisational efforts from a range of

[1] See e.g. https://www.asd.gov.au/publications/protect/essential-eight-explained.htm

players, including vendors such as McAfee, and the human and technological threat intelligence capabilities that reside in firms such as ours.

Our Position

How do government agencies become cyber resilient?

Achieving cyber resilience is a challenge most organisations continually struggle with, due to the increasingly complex, rapidly-evolving cyber threat landscape and the targeted sophistication of the modern cyber attacker. As such, cyber resilience is much more than the deployment of technology or the implementation of policies and processes; it is a commitment to a continuous lifecycle of managing risk comprising people, process, and technology, incorporating organisational culture and business drivers. It requires senior leadership engagement and support, cross functional and organisational alignment, and a clear, measurable roadmap to success.

The ASD Essential Eight (including the ASD Top 4) are a good set of foundational strategies to build a cybersecurity programme on. Whilst the implementation of the ASD Top 4 has been quoted as mitigating "over 85% of adversary techniques used in targeted cyber intrusions which ASD has visibility of," one needs to remember that the remaining 15% still represents a considerable risk exposure. In addition, this does not cover threats and attacks which may not be visible, exacerbating the issues and cyber risk exposure.

The latest Verizon Data Breach Report published in April 2017 noted that 51% of breaches involved some form of malware, which leaves 49% of breaches where malware was a non-factor. This is noteworthy as the ASD top 4 controls are malware-centric. While the "Essential Eight" mitigating strategies extend beyond malware-centricity, a holistic strategy is needed to fully address what it means to be a truly cyber resilient organisation.

At its core, cyber resilience is measured by the ability for an organisation to continue functioning at an acceptable level of service during, and after a cyber incident. It is the term "acceptable" that may vary depending on the risk profile of an organisation.

To be cyber resilient, organisations need to have clear visibility of the following:

1. Risk profile – What kind of organisation are you, and which cyber threat scenarios are you most prone to?
2. Risk appetite – To what extent is each cyber threat scenario (or cyber incident) acceptable and what are the key metrics?

3. Quantifiable risk exposure – What is your cyber risk worth? For each key cyber incident that occurs, what do you stand to lose in reputational, regulatory and financial terms?
4. Cybersecurity capability maturity – How mature is the organisation in all the relevant people, process, and technology capabilities that apply to your cybersecurity framework? What needs to be improved?
5. Gap analysis and remediation – What is your plan for addressing your gaps?

The above items should form the key parts of a cybersecurity strategy. It is through having a holistic view of cyber risks and an actionable, practical cybersecurity strategy that has been put in place, that an organisation can truly be cyber resilient.

In order to achieve this, it is important to set in place a strategy where the following questions are answered and operationalised:

1. Governance – How are you keeping track of your cyber risk and cybersecurity programme? Who are the accountable parties and how are they being measured?
2. Metrics – How are you updating, measuring and reporting on your cyber risks, threats, and quantifiable exposure? How these are being mitigated? Do you have an up-to-date view of your cybersecurity capability and maturity?
3. Continuous improvement – How are you ensuring that you are maintaining an up-to-date view of your gaps and the steps required to address them?
4. Collaboration – Are you working with your peers and service providers to ensure you have the full picture? Are you leveraging all the capability available to you efficiently?
5. Executive oversight, alignment and support – Are you ensuring your executive stakeholders are engaged with your strategy and plans? Are they supportive? Are you ensuring your incentives and metrics are aligned at all levels of the organisation and working towards a common goal?

A cyber resilient organisation needs to have a holistic plan in place and ensure it is properly executed with the right visibility, alignment and support from all levels within the organisation. In addition, the cybersecurity strategy must be iterative and dynamic because the cyber threat landscape is ever-evolving and becoming increasingly more complex. Finally, no organisation can hope to combat cyber threats in isolation. The key is to collaborate and work together with peers, supporters, solution providers, and industry groups towards a common goal in defending ourselves against a common enemy.

McAfee
Together is power.

Building an architectural platform for cyber resilience

While the “Essential Eight” (and ASD Top 4) form a solid platform to build on, a resilient defence comprises many more capabilities, and subsequently technical controls. A sustainable, resilient cyber defence is founded upon a Unified Defence Platform architecture approach. This platform is designed to address cyber threats throughout the stages of a threat defence lifecycle: protection, detection and correction.

This platform must be enabled by a layer of intelligence, automation, integration and orchestration across all connected components, delivering efficiencies by reducing discrete, manual tasks and applying security context and intelligence to make more accurate, well-informed decisions.

An extensible and open platform with a diverse ecosystem of technology capabilities is critical to achieving cyber resilience as this enables the addition or retirement of security capabilities as an organisation’s risk profile evolves, as opposed to having to acquire and implement additional, discrete controls.

Finally, specialist cybersecurity skills, capabilities and global reach can contribute considerably to the cyber resilience equation by augmenting existing operational teams. This includes global cyber threat research and intelligence, advanced consulting, implementation, operational and support services.

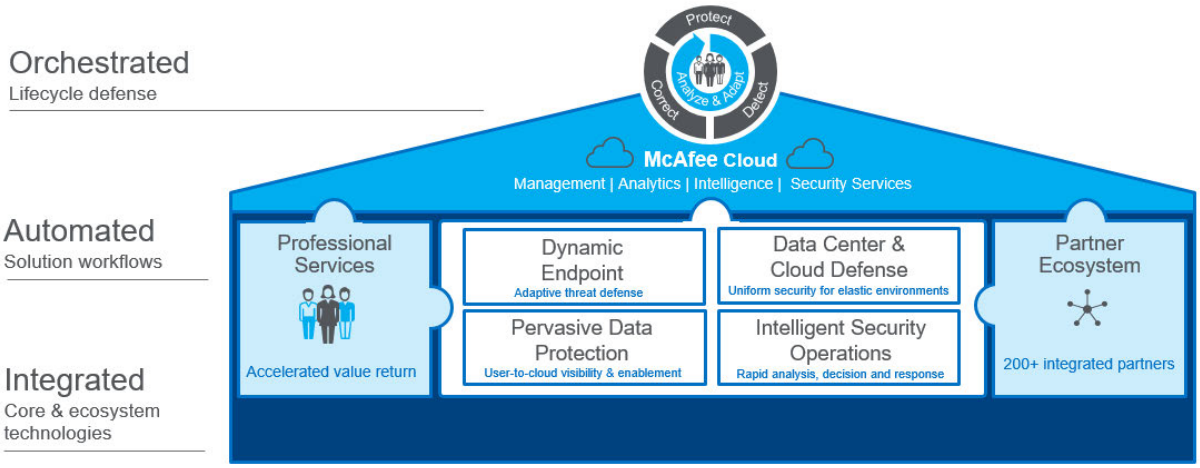

Figure 1. Unified Defence Platform

McAfee
Together is power.

Strategic recommendations for achieving sustainable cyber resilience

While subsequent sections address our views and recommendations specific to the ASD Essential Eight (and Top 4), we have outlined a few strategic recommendations that are equally important in achieving cyber resilience: –

- **Third-party Security Assessments and Penetration testing** – While reviewing implemented controls and frameworks is a key step in understanding cyber-resilience, the commissioning of ongoing active testing of cyber-defences to determine a real-world state of resilience should be included in any ongoing cyber resilience activities. These assessments should be carried out by independent, suitably qualified and experienced testing teams.
- **Establish Interdepartmental knowledge-sharing platform for control implementation** – Where departments have been successful in achieving resilience, more action needs to be taken to pragmatically share approaches taken with other, less resilient departments, and the public. Where relevant, consider using the assistance of a third-party partner with deep industry experience and capability (e.g. McAfee) to assist with facilitating forums and providing operational platforms to accelerate collaboration and sharing.
- **Reduce complexity of cyber estate** – Orchestration and automation aligning security controls contribute significantly to a cyber defence, particularly in reducing human error and alleviating the need to manually perform repeatable tasks and activities.

Whitelisting

Application Whitelisting is a very effective method of preventing malware from detonating. By only allowing trusted software applications to run, any untrustworthy application – as malware can be classified – is rendered inert and unable to cause the damage for which it was intended.

So why has application whitelisting not been more broadly implemented or often not implemented to a level necessary of compliance? The key challenge is that the whitelist – an inventory of all trusted applications allowed to run – is ever evolving due to an organisation's software deployment lifecycle, and the changing whitelist requires ongoing maintenance to ensure it remains accurate. For example, a whitelist that does not permit a new version of a trusted application from executing can cause disruption to a business by essentially causing a denial of service.

As per ANAO Report No.42 2016-17, it is imperative that an entity must have a sound entity-wide ICT general controls framework to implement a sustainable Application Whitelisting capability. We also believe that to deliver an efficient application whitelisting outcome, the application whitelisting solution must provide the following core capabilities: -

- **Dynamically maintained whitelist** - A static approach to maintaining a whitelist will result in too much operational overhead, at the cost of time and accuracy. A whitelist must be dynamically maintained by mapping to organisation change processes enabling a whitelist to change automatically in accordance with approved changes.
- **Reputation-aware** - Irrespective of change processes, applications added to a whitelist must be validated for trustworthiness. What if malware was inadvertently whitelisted? Local, community and global intelligence must be automatically applied to each application component to understand if an application should be trusted.
- **Non-intrusive deployment** - To ensure swift adoption and to minimise disruption, the application whitelisting approach must provide for running in a non-enforced state to enable visibility of change processes, and build confidence prior to enabling enforcement.
- **End-user centric** - Application whitelisting enforces change procedures and quickly highlights where procedures may be broken. End users must be adequately notified of any issues affecting the applications they are accessing and provide for swift remediation through integration with change management tools.

Application patches and Security Patches

Patching of applications and operating systems is a critical function of a resilient cyber defence. However, organisations are challenged by patching in the following ways: -

- **A patch introduces change** - Deployment of a patch represents a change to an IT asset, and consequently must be assessed per change approval procedures and quality and assurance testing. This requirement introduces patch deployment inertia and will be further complicated where system uptime is affected and/or patch deployment is complex.
- **Patches affect all applications** - All applications are subject to patches over time, and with organisations managing hundreds to thousands of approved applications the burden of patch deployment is high.

- **A patch may not exist** – A patch may not exist for a newly discovered vulnerability representing a window of exposure. Additionally, for legacy systems a patch may either not be supported or may never exist.

To augment a robust patch management program, businesses should implement mitigating controls in parallel that provide *virtual patching* of vulnerabilities. Virtual patching applies protective controls to prevent a vulnerability from being exploited. The benefit of this approach is to reduce the window of exposure to threats while allowing adequate time to validate and approve patch deployment against approved software deployment lifecycle procedures. Mitigating controls include host, network and database intrusion prevention and exploit prevention capabilities.

Managing Access Provisions for Privileged User Accounts

Privileged account access must be strictly controlled and monitored and in addition recommend: –

- **Effective privilege management should be enriched with context** – Privilege escalation and management should not be carried out in isolation of other security controls. A resilient approach should enable privilege escalation or privileged access events to consider further context such as asset criticality, data criticality and/or trustworthiness of the device or application interacting with the privileged user. This is only possible through an integrated platform approach.

Further mitigation strategies: Applying the Essential Eight

With the February 2017 announcement of the essential eight security controls, it is concerning as per ANAO Report No.42 2016-17 that implementation of the Top 4 controls has the highest rate of self-assessed non-compliance among the 36 requirements of the Protective Security Policy Framework (PSPF). The introduction of additional control considerations – if added to the PSPF – would likely increase non-compliance of departments and affect short-term prioritisation of Top 4 control implementation.

Of the additional security controls recommended in the Essential Eight, the following recommendations should be considered.

Disable untrusted Microsoft Office macros – While this is a strongly recommended approach, like Application Whitelisting this must be implemented in concert with a strong ICT general controls framework. Disabling without exception could cause valid macros from no longer working so a strong process must be defined. Where

exemptions or overrides are applied, it is important to deploy a compensating control such as an antimalware scanning engine and/or host intrusion prevention tool to analyse macros on execution.

User application hardening – Removal of high risk applications is strongly recommended. However, this is often not a simple exercise due to disparate application requirements and in some cases, legacy application and operating system support. Where a risky application cannot be removed, deployment of the following mitigating controls can assist:

- Redirection of enterprise web traffic to an advanced malware and code emulation service
- Host Intrusion Prevention and Exploit Prevention controls
- Application Whitelisting
- Endpoint application containment

Application Hardening should also be incorporated into the software development lifecycle where departments are building their own applications.

Multi-factor authentication and Daily backup of important data – These capabilities are an essential component of a resilient cyber defence. A Unified Defence Platform should have the capability to integrate these capabilities.

Our company

McAfee remains one of the most recognised and trusted brands in the security and general IT markets, with almost 30 years of continued leadership and experience in the cybersecurity arena. People around the world trust McAfee to deliver innovative solutions, and collaboratively explore and solve real-world problems, producing better outcomes for its partners and customers. With a track record for delivering excellent outcomes, innovation and stability, we are the trusted security partner for 90 of the Fortune 100, support over 125,000 corporate customers, and are present in the majority of Global 2000 firms.

We are one of the leading global firms providing an integrated, automated open security platform that increases protection, reduces response times, and maximises speed and resources, and allows our customers and partners to focus on security and business outcomes.

In the current threat landscape, we know that we need to stay agile to continue to target cyber threats. On 4 April 2017, we rebranded from Intel Security to the new McAfee,

commencing a new phase in our corporate history, and developing a whole new level of support for our clients, which includes major government departments around the world and the world's leading companies.

Intel, which acquired McAfee in 2013, retains a 49% stake in our operations, with TPG retaining a 51% stake. This makes McAfee one of the largest independent, pure play cybersecurity companies in the world. We are very excited to be taking the next step and are working actively in partnership with governments and corporations around the world.

With 7,500 dedicated cyber security professionals world-wide, McAfee is one of the world's leading independent cybersecurity companies. Inspired by the power of working together, McAfee creates business and consumer solutions that make the world a safer place. McAfee solutions deliver the highest levels of threat visibility and antimalware protection, including comprehensive system and endpoint protection, network security, cloud security, database security, endpoint detection and response, and data protection. Our complete security solutions extend beyond virus software and antimalware protection to server security, SIEM, and intrusion prevention systems (IPS).

Backed by McAfee Global Threat Intelligence, our solutions help companies enhance visibility into their security postures, allowing business to embrace virtualisation, cloud services, and mobile devices, while protecting critical assets and sensitive data, and improving incident response. We are identifying more than 500,000 new threats each day.

Our industry-leading security offerings include:

- McAfee Endpoint Threat Defence and Response: Combines machine learning analytics and behaviour-based protection with endpoint detection and response capabilities.
- McAfee Complete Endpoint Threat Protection: Advanced endpoint security with antivirus, antispam, anti-malware, device control, web security, and firewall works across Windows, Mac, and Linux systems.
- McAfee SIEM: Bringing together event, threat, and risk data, McAfee SIEM solutions provide real-time visibility into all security activities to improve compliance management and speed up incident response times.
- McAfee Threat Intelligence Exchange: Get immediate visibility into the presence of advanced targeted attacks and optimise threat detection and response by closing the gap from malware encounter to containment from days, weeks, and months down to milliseconds.

- McAfee Network Security Platform (IPS): Our best-in-class intrusion prevention system delivers real-time defences against known, zero-day, denial-of-service (DoS), distributed denial-of-service (DDoS), SYN flood, and encrypted attacks.

McAfee is committed to raising awareness about all forms of cyber threat in the community. Since 2012, McAfee (and before that Intel Security) has partnered with Life Education to raise awareness around the importance of cyber safety and the issues surrounding cyberbullying. Together we have developed and built two cyber safety modules, bCyberwise and It's Your Call, which since 2013 has had reached 365,000 students in over 8,450 schools.

McAfee's Digital Safety Program is a free initiative designed to teach students, families and seniors how to safely access the Internet. McAfee employees volunteer to educate school-aged children, parents, teachers and seniors about digital safety, digital security and responsible digital behaviour.

Contact details

For further information on our submission, please contact:

Ian Yip
Chief Technology Officer, McAfee, Asia Pacific
Level 20, 201 Miller Street, North Sydney NSW 2060
M: [redacted]