InfoTrust Response to 2023 – 2030 Australian Cyber Security Strategy Discussion Paper

A message of simplification is key

It is InfoTrust's belief that the Government should look to simplify the regulatory requirements for Australian organisations as much as possible to uplift security posture across Australia.

The ACSC defined an 'Essential 8' strategies, from a larger number of strategies to mitigation intrusion.

These strategies are all well described and the Top 4 of the essential 8 strategies are required for membership of Defence Industry Security Program (DISP) here, and include:

- Application control
- Patch applications
- Patch operating systems
- Restrict administrative privileges.

In our experience adoption of the Essential 8 can be costly and difficult to achieve for some organisations and agencies, particularly those without in-house expertise or managed service arrangements. Though the Essential 8 (and other ASD strategies) are all sound and effective practices, implementation can in many cases be cumbersome or cost prohibitive, with limited skills being available to both organisations and agencies for effective application and ongoing maintenance. For instance, application whitelisting (an extremely effective control) is relatively easy to achieve in some cases, but for many systems is an un-manageable and costly exercise.

InfoTrust advises that to quickly improve security posture across Australian businesses and the public, the Government should be looking to our Commonwealth partner, the United Kingdom, and their two-tier model implemented in 2014.

Suggestions to look at alignment with two tier model UK's National Cyber Security Centre (NCSC) has adopted.

Cyber Essentials (GCHQ)

- Five areas and core requirements for IT infrastructure are defined:
    - Firewalls –
        - Inclusions: boundary firewalls, desktop computers, laptops, routers, servers, IaaS, PaaS, Saas
        - Aim: to make sure only secure and necessary network services can be accessed from the internet
    - Secure configuration
        - Inclusions: servers, desktop computers, laptops, tablets, mobile phones, thing clients, IaaS, PaaS, SaaS
        - Aim: Ensure that computers and network devices are properly configured to reduce vulnerabilities, and provide only the services required to fulfil their role

- User access control
  - Inclusions: servers, desktop computers, laptops, tablets, mobile phones, IaaS, PaaS, SaaS
  - Aim: Ensure that user accounts are assigned to authorised individuals only, and provide access to only those apps, computers and networks the user needs to carry out their role
- Malware protection
  - Inclusions: servers, desktop computers, laptops, tablets, mobile phones, IaaS, PaaS, SaaS
  - Aim: To restrict the execution of known malware and untrusted software, from causing damage or accessing data
- Security update management
  - Inclusions: servers, desktop computers, laptops, tablets, mobile phones, firewalls, routers, IaaS, PaaS, Saas
  - Aim: Ensure that devices and software are not vulnerable to known security issues for which fixes are available

Cyber Essentials Plus

- All the above, plus technical validation of the 5 controls

UK organisations can achieve certification by completing a self-assessment and then utilising a qualified assessor to verify the information provided.

InfoTrust strongly believes that the 5 controls outlined above can easily be implemented and assessed by Australian organisations of all sizes, and the security uplift for the Australian public would be significant.

These 5 controls listed by the Cyber Essentials framework could easily be implemented by organisations of all sizes as they would not require sophisticated IT knowledge, expensive technologies, or significant effort. Additionally, the Australian government could increase the uptake of this program by making the standard a mandatory requirement when supplying goods or services with federal government departments, agencies and other businesses.

Cyber security insurance

Cyber security policies have become mandatory for some government agencies (including local councils) and organisations. With the hardening of insurance markets and large insurer losses, security insurance policy renewal amounts are increasing significantly, in some cases up to 500% and beyond. For agencies (and some organisations) the mandating of security insurance has ironically led to bigger losses for them than some ransomware demands.

We propose more careful consideration is taken in response to security insurance obligations for agencies and organisations. Taking into account considerations that improve whole of government cyber security insurance policy approaches (e.g. Victoria, Western Australia). The insurers who are underwriting the risks for security policies in Australia are not currently well equipped with the expertise or knowledge to measure and determine risk exposures for different market segments; increasing their loss ratios and the cost to the insured. InfoTrust suggests that utilising appropriate management system standards or frameworks is a more suitable strategy than requiring potentially

cost-prohibitive products, which have been seen to inconsistently provide coverage for those holding cyber insurance policies.

The NCSC offers organisations that hold the Cyber Essentials Certification at either basic or plus level free cyber liability insurance. We believe that Australia should follow this example to make cyber security insurance feasible for all. Their additional criteria are below;

- Organisation must be certified with a certification body
- Organisation turnover must be under £20,000,000