14th February 2024

2023-2030 Australian Cyber Security Strategy: Legislative Reforms Consultation Paper Response

Lead author:
Chris Usserman – Director of Security Architecture
Infoblox Federal

Corresponding author:
Tim Hartman – Head of Solution Architecture
Infoblox Australia and New Zealand

Summary

Infoblox, the leader in next generation Domain Name Systems Management and Security, thanks the Australian Government for the opportunity to provide our comments and recommendations to the 2023-2030 Cyber Security Strategy: Legislative Reforms Consultation Paper via this response.

This submission on Legislative Reforms follows Infoblox' response to the 2023-2030 Australian Cyber Security Development Discussion Paper Response as found here, which we will reference in this submission.

Elements Infoblox raised as crucial concerns were:

Essential 8 Controls: We recommend nationally adopting the 'Essential 8' controls, with defined milestones, tax incentives, and comprehensive training to boost cybersecurity.

Legislative Reforms: Enhance cyber resilience by broadening the definition of 'critical assets' and addressing nested dependencies to safeguard both physical and administrative networks.

Threat Blocking at Scale: Proposing advanced protective DNS (PDNS) solutions for automated, scalable threat blocking and advocating for a Zero Trust model. Customized PDNS solutions for different entities are suggested.

Continuous Measurement and Reporting: Stressing the need for ongoing measurement and reporting for national cyber resilience, including third-party verification and collaboration with accredited cybersecurity services.

Please find below our comments and recommendations on Legislative Reforms.

Part 1 – New cyber security legislation

As Infoblox and several other respondents highlighted in the Strategy Development Paper, and noted by the reference on Page 7, Part 1, which reads "…viability of a Cyber Security Act that harmonises a broad spectrum of domestic cyber security legislation into a unified instrument.'. Infoblox agrees and supports this approach as the laws today are too complicated for most businesses to interpret and follow.

Organisations in Australia that fall under Critical Infrastructure such as Communications, Banking and Finance, Mining, etc. Are particularly impacted by multiple regulations and standards that are either not aligned or at worst contradictory.

Measure 1: Helping prevent cyber incidents – Secure-by-design standards for Internet of Things devices

The Legislative Reforms document states, ***'As a relatively small technology market, it is critical that Australia remains in step with the international market to minimise regulatory burden for vendors, ensuring consumers in Australia have access to the same protections as their international counterparts and do not become easy targets.'***

The document speaks to UK, US, Singapore, and EU IoT standards. While Australia is considering standards, it should also leverage its Cyber Ambassador to bring the Australian government into a more dominant, requirement-generating position, rather than just wait to leverage what the rest of the international community is doing. This would amplify the Commonwealth's overall voice such that it's not just a 'relatively small technology market', but in fact, is an extension of a much larger market.

Shield #5 – Sovereign Capabilities, and Shield #6 – Resilient Region and Global Leadership, will likely cover these types of engagements that require global influencing and local ownership.

Question 1. Who in the smart device supply chain should be responsible for complying with a proposed mandatory cyber security standard?

As per the above statement about Australia taking on a greater leadership role the IoT market will require similar global participation as the NCAP (New Car Assessment Program) and Australia's ANCAP safety rating body or the ENERGY STAR rating for white goods and electrical equipment, but instead a cyber safety rating for IoT solutions commercial or domestic.

Question 2. Are the first three principles of the ETSI EN 303 645 standard an appropriate minimum baseline for consumer-grade IoT devices sold in Australia?

The first three principles of ETSI EN 303 645 grade IoT are (1) No universal default password, (2) implement a means to manage reports of vulnerabilities, and (3) keep software updated, are a great starting point and would serve Australian consumers well. While compromised IoT equipment and software or firmware infections have mostly been contained to CCTV cameras and Network Attached Storage devices, they are on the rise, and many use the same third-party componentry across many devices that would present an ideal expanding target for a threat actor.

Question 3. What alternative standards, if any, should the Government consider?

Protective DNS threat feeds, or Response Policy Zones, exist that effectively block compromised devices from contacting their Command-and-Control servers and should be considered for both blocking and alerting on compromised IoT on the network wherever applicable. IoT protection and alerting could be considered as part of an ongoing protective DNS strategy.

Question 4. Should a broad definition, subject to exceptions, be used to define the smart devices that are subject to an Australian mandatory standard? Should this be the same as the definition in the PTSI Act in the UK?

The UK PTSI Act will apply from April 2024 onwards. It holds manufacturers, importers and distributors accountable with is a voluntary code of conduct. Since it is voluntary and therefore not transparent, it

would be worth considering a similar system such as safety ratings on cars, or power consumption stickers on household appliances for internet or network connected devices.

Question 5. What types of smart devices should not be covered by a mandatory cyber security standard?

Infoblox would recommend coverage of a cyber security standard that incorporates internet or network connected devices including Ethernet, Wi-Fi, Bluetooth, Zigbee, Z-Wave and other standards used in near, peer, server or cloud connected devices and systems.

Question 6. What is an appropriate timeframe for industry to adjust to new cyber security requirements for smart devices?

Australia is considering a 12-month transition period. Infoblox believes this is more than acceptable given that IoT manufacturers must already comply with the international community's requirements. This will allow the vendors/resellers ample time to sell off product and resupply with compliant product. In addition, any product on shelf that's not compliant should be retroactively identified prior to sale as part of an obligation of consumer notice.

Question 7. Does the Regulatory Powers Act provide a suitable framework for monitoring compliance and enforcement of a mandatory cyber security standard for smart devices?

Yes, Infoblox believes it would as the regulatory powers act provides for a standard suite of provisions in relation to monitoring and investigating powers, as well as substantial enforcement provisions using civil penalties, infringement notices, enforceable undertakings and injunctions.

Measure 2: Further understanding cyber incidents – Ransomware reporting for businesses

Question 8. What mandatory information should be reported if an entity has been subject to a ransomware or cyber extortion incident?

Two things come to mind regarding ransomware/extortion incident reporting. There's not much (anything) in the reporting that helps identify victimology (location/sector/impact/etc.) If I were ACSC, I would want to know about all the events, especially if it's no-fault. If there's no harm to the business for reporting, then lower the threshold. This doesn't increase the burden on those businesses to have all the answers to their reporting questions—just answer what you can. The KEY for ACSC is VISIBILITY. They need to correlate sector, geographic, and relative impact to the Commonwealth for opportunistic vs targeted attacks. So, 1) lower reporting threshold, and 2) require non-punitive victimology identification and characterisation.

Question 13. To what extent would the no-fault and no-liability principles provide more confidence for entities reporting a ransomware or cyber extortion incident to Government?

On the punitive/non-punitive side of things: consider COVID, Flu, or any other physical virus. If a person takes all the necessary precautions and still contracts a virus, we don't hold them accountable. So, a

business should not be held accountable, generally, unless they're in a critical sector AND they fail to meet the minimum standards which would fall under regulatory oversight anyway.

Question 14. How can the Government ensure that the no-fault and no-liability principles balance public expectations that businesses should take accountability for their cyber security?

On the limited use/safe-harbor consideration: it's critical that actionable/defensible information be shared with the cybersecurity community. That does NOT have to include attributable victimology. Regulators should only act on the applicable standards and requirements when interacting with an entity, and may ask the regulated about any cyber incidents, including relevant post-mortem questions—i.e. impact, how long to remediate, etc. ACSC/ASD should provide industry and regulators with generalised attack methodologies that aid in developing/refining sector-based cyber requirements. These should be living requirements wherein the law establishes the oversight authority and regulated requirements, but the specific requirements themselves are communicated with an expected implementation timeline. In the US military, they're called cyber tasking orders (CTOs) where organisations are required to act within a set timeframe. CISA just issued an emergency directive in February 2024 to disconnect all Ivanti VPNs from operational networks due to ongoing 0-day exploitation. Commonwealth organisations would be required to comply with CTOs and ACSC emergency directives. It would be up to the regulators to ensure those directives were complied with.

Measure 6: Improving our national response to the consequences of significant incidents – Consequence management powers

Question 37. How would a directions power assist you in taking action to address the consequences of an incident?

The directions power would provide the necessary authoritative and structured framework enabling coordinated and timely responses to cyber incidents that meet or exceed defined criteria. The directions power would enable:

Standardised Response: Establishment of procedures and protocols for cyber incident response, like other emergency response plans, provides clarity of purpose and ensures a unified approach across entities. This would enable our organisation to support the government's actions more effectively.

Rapid Mobilisation: It would enable the government to mobilise public and/or private resources to respond to cyber incidents, thereby rapidly aiding a victim organisation's response and recovery.

Impact Mitigation: The enacting of response plans, or parts therein, the directing body's actions can help in promptly mitigating incident impact, limited damage to critical infrastructure and services, and reduces recovery time. This is especially important for less cyber-mature organisations that may otherwise face uncertain fate, lack clarity of direction, or inability to take executive action (make decisions).

Legal Authority: Directions power gives legal backing to actions taken in response to cyber threats, absolving those involved in the response efforts from potential legal repercussions, assuming those actions are taken within the permissible bounds of the response plans.

Financial Backing: A federal directions power that mobilises state, territory, and/or private entity resources should account for financial coverage of those resources for the duration of the directions power authority, or until that resource is relieved of federal service.

Question 38. What other legislation or policy frameworks (e.g., at a state and territory level) would interact with the proposed consequence management power and should be considered prior to its use?

Most states and territories have their own emergency management frameworks, which may also include cyber incidents. Evaluate how a national cyber emergency plan would supplement, complement, or supersede regional plans. Also consider the regional resources available should direction powers be implemented. Further considerations for interaction:

Existing Privacy Laws: Federal and state/territorial laws may already dictate how personal information is handled during incident responses, e.g. handling PII during large-scale medical emergencies.

Critical Infrastructure Protection Laws: The Security of Critical Infrastructure Act of 2018 and similar state-level legislation already provide mechanisms for protecting critical infrastructure. These laws may already be closely aligned with the directions power. OBJ

The Telecommunications Act of 1997 and the subsequent Telecommunications and Other Legislation Amendment Act 2018: While the former is the cornerstone of the government's authority, the latter amendment better provides for "cyber" incidents while also balancing governmental authority and personal privacy.

Question 39. What principles, safeguards and oversight mechanisms should Government establish to manage the use of a consequence management power?

The use of consequence management powers should be governed by the pre-established principles and safeguards that ensure accountability, transparency, and protection of civil liberties. Consider the following:

Oversight: An independent body, composed of vetted public and private representation, should oversee the use of these powers. This oversight committee would have the same, or similar access and authority as other governmental oversight committees.

Transparency: Clear guidelines on how and when the power can be implemented and used, limitations, who has the authority to enact, and disclosure on the use of said powers to the public or responsible oversight body.

Privacy Protection: Measures should be defined and enacted to ensure that the privacy of individuals and organisations, and their data, is protected in accordance with existing law(s).

Proportioned Authorities: Actions taken under a consequence management power should be measured and proportional to the threat and potential impact, avoiding broad powers. For example, consequence management power in response to a cyber-attack should not extend to physical port security (i.e. enhanced explosive detection inspections) unless there's justifiable cause. (See Oversight, Transparency)

Review and Retirement: Implement regular reviews of the power's effectiveness and include expiration/retirement clauses by some or all the authorities to ensure they are only enacted for as long as reasonably necessary.

Measure 9: Consolidating telecommunication security requirements – Telecommunications sector security under the SOCI Act.

Question 45. What are the main barriers to engaging with government through the notification process as it is currently enforced? How can the obligation to notify be clarified?

Infoblox tracks many regulatory developments across the globe, with a focus on threat blocking and notification. Drawing a parallel to the recent changes in notification requirements to the SEC in the United States for publicly listed companies. Further defining and refining them triggers that would require notification. For example; the Securities and Exchange Commission (SEC) that governs all business reporting requirements for publicly traded companies on the stock market, just put in place a rule that says, in part, that if you're a publicly traded company and you suffer a cyber incident, you must officially disclose it to the SEC (which makes it public record) within four days IF it could materially affect the stock price. Meaning, if a cyber incident is going to cause the stock to drop more than average daily movement, it must be reported.

Now, this only applies to companies that have are traded on the stock market, but a similar aspect could be considered. For private entities that provide a critical service, hold customer data, or are of/above a certain revenue stream should also report.

About Infoblox

Infoblox is the leader in next generation Domain Name Systems Management and Security at scale. More than 12,000 customers, including over 70 percent of the Fortune 500 rely on Infoblox to scale, simplify and secure their hybrid networks to meet the modern challenges of a cloud-first world. The Infoblox cyber intelligence unit creates, aggregates and curates information on threats to provide actionable intelligence that is high quality, timely and reliable. Threat information from Infoblox minimises false positives, so you can be confident in what you are blocking, while ensuring unified security policy across the entire security infrastructure. Infoblox Federal is a cleared US contractor supporting the US government, FIVE EYES, and public sector entities.

infoblox.

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com