Impunity to fight cyber attacks: New laws

Denham Sadler, Senior Reporter,12 August 2020

Private companies running nationally significant systems will be given legal impunity to fight cyber threats, while the federal government will be allowed to take control of these companies in the face of a serious threat, under proposed new laws.

Reforms to protect Australia's critical infrastructure and systems of national significance with positive security obligations, enhanced cybersecurity obligations and government assistance, were key planks of the federal government's 2020 Cyber Security Strategy, unveiled last week.

The changes aim to uplift the security and resilience of critical infrastructure through a collaboration with industry to protect against the potential for "cascading consequences across our economy, security and sovereignty", such as the destruction of essential medical supplies, impact to water supply or the shutdown of telecommunications networks.

Cyber force: Sweeping new powers put forward to protect critical infrastructure

The Department of Home Affairs has released a discussion paper on the planned legislation, outlining a range of new obligations to be imposed on an expanded list of critical infrastructure sectors.

The new rules would apply to some private companies operating in sectors that include banking and finance, communications, data and the cloud, defence industry, education, research and innovation, energy and space.

"The services that these sectors provide are crucial to Australia's economy, security and sovereignty. It is essential that critical infrastructure entities within these sectors take a proactive approach to security and resilience," the discussion paper said.

"Mature sectors will benefit from an uplift in their supply chain, as well as the networks and systems that they depend on," it said.

The paper outlines how government would step in to protect critical infrastructure when there was an "imminent cyber threat or incident that could significantly impact Australia's economy, security or sovereignty".

The government would provide "reasonable, proportionate and time-sensitive directions to entities" to minimise the impact of the cyberattack, and the entity can request that this be done.

The new laws would also give critical infrastructure operators the power to bypass any relevant laws in order to protect against a cyberattack.

“Entities must be empowered to take necessary, preventative and mitigating action against significant threats. Government recognises that entities require appropriate immunities to ensure they are not limited by concerns of legal redress for simply protecting their business and the community,” the discussion paper said.

The paper states that “under no circumstances” would operators be directed or authorised to take actions against the perpetrator, such as a “hack-back”.

If the federal government itself identified an “immediate and serious cyber threat” against a piece of critical infrastructure, it would be given the power to declare an emergency and take control of the systems and networks to take direct action.

“These powers would be exercised with appropriate immunities and limited by robust checks and balances. The primary purpose of these powers would be to allow government to assist entities take technical action to defend and protect their networks and systems, and provide advice on mitigating damage, restoring services and remediation,” the paper said.

The threat would be judged on its potential consequence to the Australian economy, security and sovereignty, its likelihood to spread across jurisdictions and its level of imminence.

Critical infrastructure operators would mostly allow this to happen voluntarily, the government said, but the government would also be legally able to do so without permission.

“There may be cases where entities are unwilling to work with government to restore systems in a timely manner. Government needs to have a clear and unambiguous legal basis on which to act in the national interest and maintain continuity of any dependent essential services,” it said.

The consultation paper also covers the positive security obligations to be imposed on critical infrastructure owners and operators and the enhanced cybersecurity obligations, mostly focusing on cooperation with the government.

“A range of hazards have the potential to significantly compromise the supply of essential services across Australia; physical, personnel and cybersecurity are all increasingly interrelated. We must work together now to ensure Australia’s security practices, policies and laws bolster the security and resilience of our critical infrastructure and position us to act in any future emergency,” the discussion paper said.

“We need a better shared understanding of the threats we face and how we can combat them. Together, owners and operators of critical infrastructure, academia and all levels of government must collectively take steps to protect Austraians from an attack and other disruptions.”

The designated entities would be subject to a set of high-level, sector agnostic principles to protect from broad hazards, along with more sector-specific guidelines. At a minimum, operators and owners of critical infrastructure will be legally obliged to identify, understand and manage any risks that may impact business continuity, mitigate these risks through proactive risk management and minimise the impact of any realised incidents.

These include specific guidelines for cybersecurity, which cover the identification and assessment of sensitive information, safeguarding this information from common and emerging cyber threats and ensuring the systems and personnel can detect, understand and respond to any potential incidents.

The government is looking for an appropriate regulator to enforce these new rules in each sector, which would be done through “flexible administrative measures and graduated enforcement powers”.

The enhanced cybersecurity obligations would only apply to particularly critical entities where there is a need to build an active partnership with near real-time information sharing, the discussion paper said.

The federal government plans to establish a system for sharing information on cyber threats with the relevant owners and operators to create a “near real-time national threat picture”. This would be fed information from industry and commercial partnerships incident reporting, cross-sectoral dependency projects, open source information and government intelligence.

“A near real-time threat picture, including intelligence insights and trends, will empower owners and operators of systems of national significance to take appropriate and timely action on their own systems,” the paper said.

“It will also provide the government with an aggregated threat picture and comprehensive understanding of the risks to critical infrastructure. This will better inform proactive and reactive cyber response options.”

Owners and operators would initially voluntarily provide information if they wish to test the system, before they become obligated to provide information about their networks and systems upon request from the government, under the planned reforms.

Submissions on the discussion paper will be accepted until 16 September, and Home Affairs has planned a number of virtual town halls and industry workshops on the issues.