

Aussie Infrastructure needs to be more Cyber Secure

If the lights go out, or the water is contaminated, who do we blame? Can we blame the Government, can we blame our aging infrastructure? No matter who you may conclude is to blame, we are still left to solve the problem. How can we make Australian Critical Infrastructure Cyber secure? How do we safeguard our economy and our lifestyle? Do we have to replace everything to be comfortable we are safe?

The North American Electric Reliability Corporation (NERC) is a non-profit corporation formed on March 28, 2006. NERC's purpose is to promote the reliability and adequacy of bulk power transmission in the electric utility systems of North America. NERC's mission states that it is to "ensure the reliability of the North American bulk power system."

The standards developed and applied by NERC are now a mature set of guidelines on how all critical assets should be operated to ensure availability to the consumer and to protect the greater economy and safety of a nation.

Critical assets are operated with commercial interest and have a competitive tension with essential service provision. This is why government regulation is required, to strike a balance and also keep those prices under control.

Lagging Aussies

The Attorney-General has released an exposure draft of the Security of Critical Infrastructure Bill, which seeks to manage the complex and evolving national security risks of sabotage, espionage and coercion posed by foreign involvement in Australia's critical infrastructure. The Australian government is currently seeking views on the draft Bill. Ultimately a critical infrastructure assets register will be used in concert with new legislation to better control high-risk sectors.

Australia's critical infrastructure can be summarised under the following categories:

- Electricity generation
- Electricity transmission/distribution
- Ports
- Water

What is the Aussie landscape

The Australian power and water infrastructure is expansive and significantly distributed, supporting the population living in coastal regions. Vast telecommunication networks are required to connect devices thus reducing the cost to operate and maintain the assets. Due to this sunk investment and despite many arguing Aussie assets are already antique, in many cases the devices for managing our networks are already "well connected", meaning the reason we have a cyber security risk is because they are in fact already on the grid! So now that is put to the side, the matter of security can be dealt with using well established standards and mature products already deployed around the world. Though these products are typically applied to Power Networks in general, the same principles apply to all critical assets extending it further to include transport and other big industry that could be orchestrated to cripple an economy.

Starting Late Isn't all Bad



Starting a race late is never good. As a consequence of NERC focusing on electricity supply to North America, industry has developed products to support the management of devices which control "the grid". Though we rarely apply this offshore standard by intent, it means Australia does not have to reinvent the wheel to roll forward in the race to better infrastructure security. The application of these standards extend beyond networks into [SCADA Software and Enterprise Information Systems](#) used for managing grid devices.

Is it time to restart or join the race in terms of standards and regulatory compliance? If Australia wants to operate in the era

of global connectivity then it needs to be prepared to accept the security baton from teams that have already run the first legs. We can join the Critical Infrastructure Cyber Security race where all the action is instead of starting way back at the beginning with no hope of ever catching up. We cannot remain hiding, because we are already globally connected, and we are already way behind. I say; adopt, adapt, move onward and upward!



[...read more](#)

References

<http://www.subnet.com/solutions/nerc-cip.aspx>