# ENERGY

Sector Overview

The energy sector is critical to Australian society, given technology's dependency on it to function. However, as the digitalisation of energy systems and networks accelerates, so do the cybersecurity threats, vulnerabilities and associated challenges confronting energy infrastructure owners and operators.

Ransomware, Remote Access Trojans (RATs), Distributed Denial of Service (DDoS), and Business Email Compromise (BEC) attacks are among the most common attack techniques employed against the energy sector. The most notable energy sector cyber incident in recent memory was the 'Colonial Pipeline' attack, which accelerated both policy and technological cyber responses in America. This ransomware attack, executed by the threat group "DarkSide", involved a single leaked password, which enabled the attackers to gain access to Colonial's network. This attack had the "real world" impact of shutting down Colonial's operations, leaving thousands of businesses and households without access to fuel.

These events remind us of the criticality of ensuring Australia's energy sector is prepared to defend its assets against cyber threats. As with all infrastructure services, the energy sector must prioritise refreshing ageing physical infrastructure, adopting digital transformation and the security investment required to protect their assets, and ensure ongoing supply for the nation.

The energy sector has a mature level of cyber security assurance compared to other SOCI-prescribed sectors, with the Australian Energy Sector Cyber Security Framework (AESCSF) used as the primary mechanism for evaluation. The initiative was expanded to cover gas markets, electricity grids, and markets not operated by the Australian Energy Market Operator (AEMO) in 2021 and liquid fuels in 2022.

The global evolution of 'smart city' initiatives to improve energy conservation and efficiency is driving innovation and the use of energy-efficient technologies. The increase in digital technology use improves energy systems' connectivity, efficiency, reliability, and sustainability. However, these advantages bring a range of new threats, amplified by the interconnected nature of energy infrastructure. This introduces supplier concentration risks across critical infrastructure sectors reliant on predictable energy delivery.

**Vulnerabilities**

As smart grid networks introduce improvements and better capabilities to the traditional electricity network, the nature of cyber threats becomes more complex and prone to new forms of cyber-attack. Any security flaws in new smart grid technology could allow hackers to access networks, compromise the confidentiality and integrity of transmitted data, and impact availability by disabling services.

Smart grid technology gives rise to new data-centric threats relating to customers. For example, smart meters capture vast amounts of user data and send it to utility owners, managers, customers, and third-party service providers. Increased adoption brings more

intelligent components used to manage network demand and electricity supply that attackers can exploit. Smart sensors can be compromised to act as primary network access vectors, and the increasing complexity of these systems poses new and unique challenges to defenders.

In contrast to the conventional electricity system, smart grid networks have numerous components outside the energy utility's boundaries. This expansion of the physical asset footprint increases the threat of unauthorised physical access being leveraged to access electronic systems.

The building of new smart grids on top of traditional energy infrastructure means that legacy equipment is likely to still be in use and, due to incompatibilities with newer technologies, may expose additional weaknesses that attackers could look to exploit.

**Types of attacks**

The ongoing digital transformation of Critical Infrastructure narrows the convergence of IT, OT, and IoT systems, which complicates the potential attack surface and vectors that may be exposed. A general lack of separation between different IT/OT/IOT networks enables attackers to compromise one system and move laterally to others based on their desired objectives. To combat these threats, solid security design principles and timely information on relevant threats are key to staying ahead of attacker techniques.

Attackers employ a range of techniques against energy infrastructure. However, these can be grouped into three main categories: *components, protocols*, and *topology*.

- Field components such as Remote Terminal Units (RTU) are often a target of attacks. Engineers typically utilise RTUs to remotely configure and troubleshoot smart grid equipment and are vulnerable to attacks where the control of devices is seized to cause malfunctions or shutdowns.
- Protocol attacks use techniques aimed at packets and false data injections to attack the communication protocol itself.
- Attacks that target the topology of a smart grid use Denial-of-Service (DoS) techniques to prevent operators from seeing the entire system, which may inhibit decision-making.

Malware threats are also relevant to smart grid technology. Attackers can create malware and distribute it to infect company systems or smart meters, with may cause outcomes such as sensitive data being exfiltrated to unauthorised systems.

**Other types of attack include but are not limited to:**

Access via database links: Control systems reflect their logs into the business network after recording their activities in a database on the control system network. A skilled attacker could access the business network database through improperly designed database management

systems and then utilise their expertise to target the control system network.

Compromising communication equipment: An attacker may compromise communication equipment, such as multiplexers, attacking them directly or using access to maintain persistence via a backdoor to launch future attacks.

**Attacks on the energy sector in Australia:**

- In 2021, the Conti ransomware group attacked the corporate ICT network of Queensland Government-owned electricity generator CS Energy. CS Energy produces 10% of the electricity for the national electricity market.
- A cyber-attack on Energy Australia compromised the personal information of hundreds of customers. Unauthorised access to the online platform impacted 323 residential and small business users.
- Chinese state-aligned threat actor TA423 (also known as Leviathan/APT40) represents a persistent cyber-espionage threat against nations and organisations operating in the South China Sea, including companies engaged in an offshore wind farm in the Taiwan Strait. TA423 attacks employed malicious emails to spread "ScanBox" malware for reconnaissance, posing as Australian media outlets. The espionage campaign ran from April to June 2022. TA423 used the information it gathered to profile victims and attack specific targets of interest with additional custom malware. TA423 is suspected of conducting multiple intrusions in Australia, Europe, and the United States as part of its intelligence-gathering and espionage goals.

**Responding to threats against the energy sector in Australia:**

Most energy sector entities won't be able to share 'machine to machine' intelligence, so an industry partner is needed as the enabler/facilitator for cyber threat intelligence (CTI) and collective defence via other means. By taking on the role of the trusted advisor/facilitator for the intelligence exchange, an industry organisation would ensure the overall quality of information flowing through its systems and out to the CI members.

'Forewarned is Forearmed', and by joining a trusted cyber community of Critical Infrastructure owners and operators responsible for protecting their energy infrastructure assets, you can join the movement to share contextual intelligence and proactively approach cyber defence. Cyber threat activity shared into the CI-ISAC ecosystem by one member has the potential to help others across the sector and the broader CI community stop similar attacks before they impact operations.

CI-ISAC, as a not-for-profit, member driven organisation, with a mission to serve its members and in turn their customers by building a trusted community and leveraging the best technology in its intelligence platform, and drawing on resources and resilience through its industry peer-to-peer network to anticipate, mitigate, and respond to cyber threats.

More information on CI-ISACs sovereign intelligence-sharing capability can be found on the official website: https://www.ci-isac.com.au , or by emailing info@ci-isac.com.au.

**Published:** 10th February 2023