COMMUNICATIONS

Sector Overview

How many times a day do you look at your mobile phone for email, instant messaging, or entertainment? Research suggests that the average Aussie checks their phone an average of 7.8 times an hour - that's almost once every 8 minutes. Any cyber-attacks on communications sector infrastructure will likely have negative operational impacts, with such impacts likely noticed almost immediately by many Australians.

Before the Internet, Australians living on an expansive landmass often felt a sense of relative isolation from the rest of the world and its troubles. However, modern communications infrastructure and technologies have made most Australians feel a greater sense of local and global connectedness, with reliable communications becoming an essential component of everyday lives.

The downside is that the increased connectivity brought once-distant threats closer to home. At the same time, the same modern communications infrastructure delivered national resiliency, enabling the nation to have an almost seamless transition to remote work in response to a global pandemic. This communications revolution occurred within a generation thanks to infrastructure largely built by cable and telecom companies, satellite providers, and internet service providers.

There are only a few dozen (35) telecommunications companies in Australia. This relative concentration of asset owners/operators and their interconnected nature represents a critical dependency for the sector itself, increasing threats to other interdependent sectors. Ultimately this means a successful cyber-attack on communications infrastructure could have significant and widespread spillover effects, making communications infrastructure an ideal target for attackers hoping to cause maximum damage and impact.

The increasing economic importance of the communications sector is reflected in its sheer size (valued at $20.2 billion; 2021) and its compound annual growth rate (CAGR) of more than 1% (2021-2026). The Australian Government's national broadband network (NBN) project is the primary driver of infrastructure expansion to meet the rise in demand for high-speed fibre broadband services and 5G services. This expansion of the 5G network is being delivered primarily by major communications players like Telstra, Optus, and Vodafone, of which Telstra remains the nation's largest by market share (43.3%).

The ability to communicate via phone, internet, wired and wireless connections depends on the telecommunications infrastructure operating reliably and without interruption. For simplicity, we can think of this infrastructure in two main clusters: fixed line and wireless networks.

In general, fixed-line usually refers to physically wired networks, or traditionally a connection provided by a cable to connect users of devices with one another. Fixed line networks still play a significant role in supporting telecommunications services that can be described as backbone infrastructure. Like any infrastructure, fixed-line networks are susceptible to disruption by natural or human-induced physical or cyber incidents and eavesdropping.

Wireless networks leverage radio frequencies to enable the transmission of data and have evolved to become the primary networking technology adopted by users. Despite not needing cables to the consumer/enterprise device, wireless networks are still dependent on multiple infrastructure layers to function, including the erection of towers, antennae, rigging, power installations, and fibre optic installation, testing, and maintenance.

Key Cyber Security Issues:

Despite the usability benefits, the lack of physical barriers protecting wireless networks makes them vulnerable to unlawful interception, eavesdropping, hacking and a range of other cyber threats, with the following are examples of cyber-attack being most common in the communications sector:

- **Denial of Service Attacks** – involve an attacker flooding a network with messages that affect the availability of network resources, which can interrupt service. Distributed denial of service attacks (DDoS) can disrupt services to millions of consumers, impact business operations, and result in significant financial losses.
- **Spoofing and Session Hijacking** – involves an attacker gaining access to network data and resources by assuming the identity of a valid user.
- **Eavesdropping** – is when unauthorised third parties intercept data transmitted over a connection.
- **Supply chain threats** – Communications companies, particularly mobile operators, typically rely on third-party suppliers to support their infrastructure. Threats may be introduced into their supply chain via these third-party providers. The 2021 SolarWinds hack is a recent example of a single supplier impacting thousands of downstream entities.
- **IoT threats** – Attackers use the Internet of Things (IoT) devices as a network entry point. They may use the same technique/vector to attack multiple devices, downloading more malicious code as they move through the network. Initial access vectors can include weak credentials, vulnerabilities, and exploit kits. Compromised IoT devices can also be leveraged to form part of botnets to launch DDoS attacks.
- **Vulnerabilities in network devices** – Routers and other network devices are prime targets for attacks against telecommunications infrastructure.

The huge volumes of data travelling over communications networks and the potential such networks represent to attack a wide array of infrastructure types make communications companies and their infrastructure a popular target for cyber attackers. Energy, information technology, and transportation sectors are just a few that depend heavily on communications sector networks.

Many communications providers won't have the capability 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 communications 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: 2nd February 2023