# In This Era '*Data is Wealth*'

The critical nature of cybersecurity in infrastructure can be highlighted by the Volt Typhoon incident in Guam, a tiny American territory with its expanding airfields and ports. In mid 2021 Volt Typhoon invaded the island's communication system quietly, compromising the systems over time including communications, energy installation, water facilities and transport system. "*Places like airport has potential value for spying as it can be used to track people in transit*", as per **The Economist** – June 15, 2024, issue. Penetrating critical infrastructure by cyber-means such as airports can have a drastic effect as it will disrupt the port control systems, communication, and air-traffic control.

Stuxnet attack invaded the Iranian nuclear facility slowly via USB sticks. Since it was an unexpected attack and was only detected when systems started to hinder and crash one after another. This puts the importance of the continuously upgraded cyber prevention. This emphasizes the importance of regularly updating risk assessments and incorporating the latest threat intelligence to prevent such attacks. As cybersecurity threats evolve, staying current with trends and best practices and regularly reviewing and updating incident response plans are crucial.

Volt Typhoon directed attack through ordinary routers, firewalls and other equipment used in offices. As a result, FBI disrupted hundreds of ageing routers which were being used to stage attack. This demands a better defence in the critical sectors such as aviation. **Paul Nakasone**, head of **NSA**, stated that "*Nations should not seek to exploit the personally identifiable information of others*". But this too is a grey area. Cyber norms remain blurry. It is important to secure the networks because by the time the intrusion is detected it might be too late to rip out cables from the back of the computers.

This calls for enhancing cyber security readiness. As **Louie Orbeta**, Manager Cyber & IT at WAA, states in his writings "*staying current with the latest trends and best practices is essential as cyber threats evolve and regularly reviewing and updating incident response plans*".

Sources:
The Economist
ColdFusion