What are the Risks to AtoN?

Are you using technology to access and share sensitive personal or business information?

If so, it is important to understand how to best protect yourself and your organisation.

Compromise can occur in the following ways:

1.

The Technology Itself

PSTN, RF, GSM, Bluetooth and Zigbee all operate on open networks and are heavily used to transfer short or long-range data. Open networks are unsecure allowing anyone to intercept, decode and use the data to their advantage. This also places the systems connected to them, more susceptible to cyber-attack.

GSM   Bluetooth   WiFi   PSTN   Zigbee
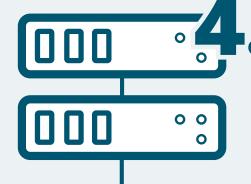(Mesh Networks)

2.

Accidental Risk

Can be the result of human error, where assets are configured incorrectly, or as a result of automated software updates. Without prior testing of the impact, a triggered update can scramble data, take systems down, deactivate assets or report inaccurate information. Reversing the update can be both time consuming and costly.

3.

Connectivity Risk

A result of network interference, where people operating on the same frequency can inadvertently or maliciously take systems down.

4.

Data Management Platforms

These systems hold organisational and user data for potentially hundreds of assets. They are often accessed by many personnel who may have out of date software or security protection.

What can Businesses do to Safeguard Themselves?

Step 1 Ensure that the organisation develops a formal cybersecurity strategy and IT policy. Ensure these policies are revisited as frequently as needed.

Step 2 Make it compulsory for all staff and contractors to action your IT policy. In particular, those who have access to your data management systems.

Step 3 Undertake a full risk assessment of the data management system, identify any possible entries for a breach and rectify.

Look out for our upcoming blog that will provide you with 'Key Design Parameters' that should be factored in to ensure robust security of 'Data Management Systems'.