2022 / White Paper

Star2M
INNOVATIVE COMMUNICATIONS

Introducing Technology Risk

How this Relates to Aids to Navigation

iridium®
connected

A cyber-attack due to inadequate or outdated security provisions can compromise the safety of personal identity information (PII), take systems offline, and can completely disable business operations.

Cyber engineering looks at the design, implementation, maintenance and improvement measures to protect the integrity, confidentiality and availability of systems and information.

Digital Technology in the AtoN Industry

Technology has transitioned over time to become a key enabler for managing Aids to Navigation. The use of portable devices to access information on-demand, whilst convenient is not without its risks.

Inadequate or outdated security provisions at a business, systems and user-level can have dire consequences. An attack can compromise the safety of personal identity information (PII), take systems offline, and can completely disable business operations.

Most organisations will have already considered the risk and importance of a cybersecurity strategy. Cyber engineering looks at the design, implementation, maintenance and improvement measures to protect the integrity, confidentiality and availability of systems and information.

For organisations that do not have a formal strategy in place, it has never been so critical to assess their level of vulnerability.

The Time to Act is Now.

Why Cybersecurity is a Must

Cyber-attacks on businesses are becoming more prevalent and particularly in the last 10-15 years, the instances of data breaches and exposed records has grown significantly. Cybersecurity company Varonis compiled **over 100 statistics and trends for 2021** that help identify the need for stricter measures.

The sectors that are the greatest targets are:

- Energy
- Transportation
- Mining
- Construction

These industries are lucrative for attackers and that is why cybersecurity is a must for organisations operating in these markets.

Even some of the largest and technically savvy organisations (Facebook, Microsoft, Yahoo) have publicly acknowledged being hit by malware. These attacks can be through rouge hacking groups, or even sanctioned by governments; to disrupt or disable operations, gain access to personal data/credit information or for a ransom.

The issuing of ransomware to initiate a system lockout is one of the top reasons behind an attack. The primary motive is to extort money. Disrupting services is a secondary aim. Unlike other industries, in the maritime industry, the probability of a terrorist attack is deemed to be relatively low, however as the industry moves towards automation, the impact could be much more significant.

OT and IoT Convergence -What this Means for the Safety of Data

Operational Technology (OT) and SCADA systems have traditionally been the means for accessing monitoring data. They were essentially silo systems that captured and relayed data for a specific business purpose.

Monitoring types include:

- Public Switch Telephone Network (PSTN) via dial-up interfaces to initiate alarms. This was instrumental to the industry in the 1980's and 90's.
- RF became popular in the early days as a last mile solution. It found its place where the PSTN networks could not service. It requires regulatory approval in most countries except for the ISM band. It is still heavily used today.
- GSM is a reliable service; however, it still has limited coverage in many areas and is subject to a technology refresh cycle.
- Bluetooth and Zigbee are used for short range connectivity options and still popular for communication to sensors and ancillary devices.
- Satellite has become more price competitive and the technology has advanced at a rapid rate. Offering truly global coverage is the preferred option for remote or offshore locations, and where GSM service is unreliable.

The popularity of the Internet of Things (IoT) over the past twenty years is changing our behaviour and the means in which we communicate. Access to Apps, data and functionality is at our fingertips and has continued to feed our growing appetite for an increasingly connected world.

The high consumer demand has driven OT providers to rethink their strategy of silo systems and move to the same IT networks used by IoT. The result is a hybrid technology network with open protocols, has public access and as such is at a high risk of being compromised.

Risk to AtoN – Why?

The use of the technology itself is a risk. Known hacks have the capability to scan and intercept data and devices. GSM, Bluetooth, PSTN, WiFi, TCP and RF all serve their purpose but are all open networks that allow for anyone to intercept, decode and use the data to their advantage. This makes these networks and systems connected to them, more susceptible to attack.

Accidental risk can be subject to the human factor, whereby assets are incorrectly configured or accidentally switched off. Automated software updates can corrupt data and completely take down a system, deactivate assets or misreport information.

Connectivity risk can result from network interference, whereby a person operating on the same frequency can take down the network, a risk that is impossible to avert.

In relation to Aids to Navigation, data management platforms are ideal for consolidating messages into a single hub, but are the most susceptible to risk of a cyber-attack. Organisations with hundreds of assets and with many personnel accessing these systems, insufficient or outdated security protocols can lead to a serious security breach.

Key Design Considerations

Key design considerations for a data management system should include:

- A minimum of AES-256 encryption and SHA-256 data protection for hashing to protect personally identifiable information (PII) and asset data.
- Segregation of PII and configuration data from asset data.
- Utilize multi-factor authentication for users (MFA), enforcing complex passwords, frequent password updates.
- Ensure the "Active Directory" is not publicly accessible.
- Create access layers to separate the database, API, front-end systems.
- Enable end-to-end encryption for users – SSL/TLS certificates.
- Conduct penetration testing continuously to help understand ongoing network threats.
- Backup and restore data management policies to mitigate chance of loss.

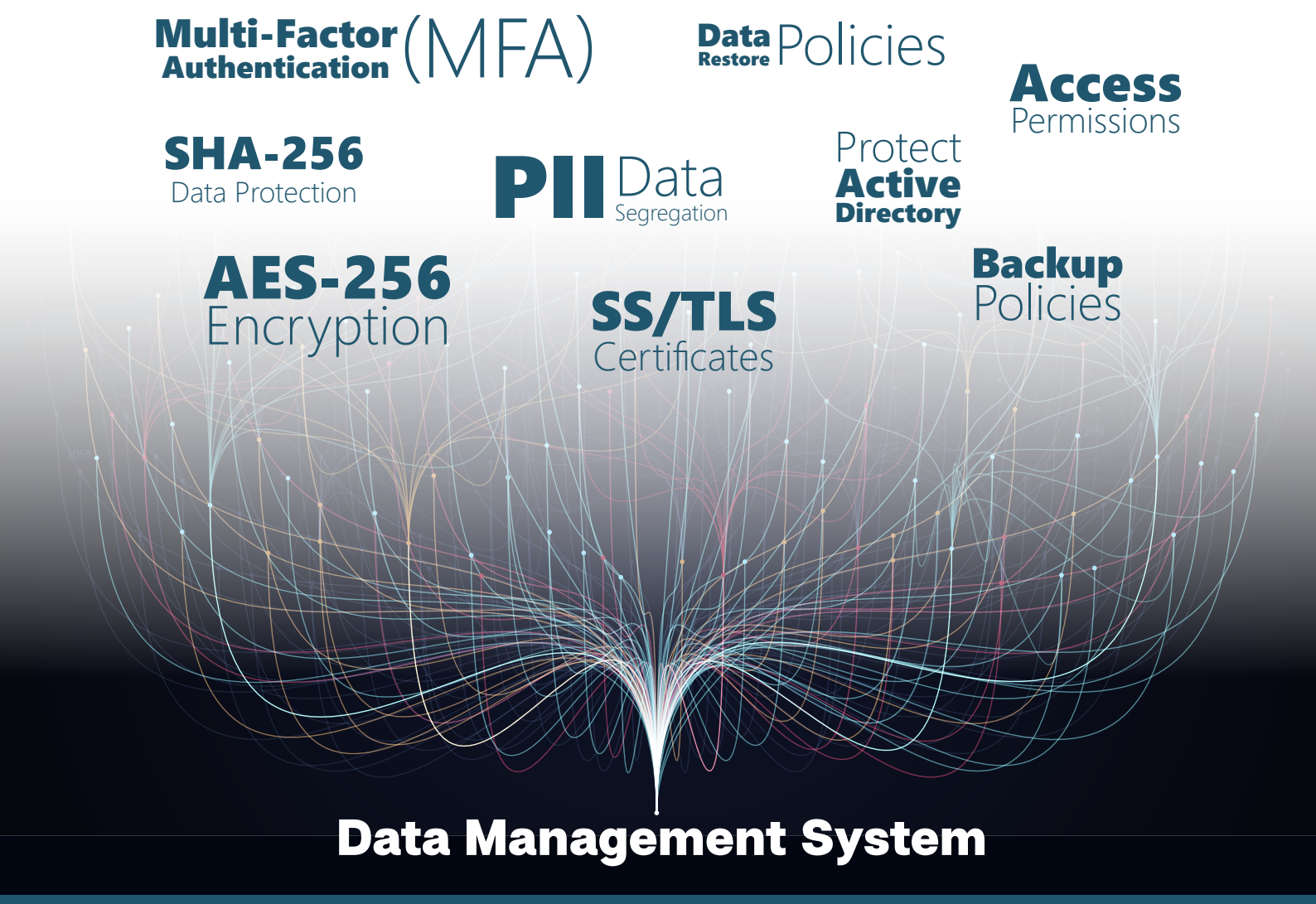
Planning for the Future

The biggest risk to organisations is their data systems and as cyber-criminals become more sophisticated, the threat of attack and it's cost to business will continue to climb.

To best mitigate the risk, it is recommended to:

- Develop a formal cybersecurity strategy and IT policy – apply and revisit as frequently as needed.
- Undertake a risk assessment of the data management system - to help to address possible entry points for a breach and develop an action plan should an intrusion occur.

For now, due to lagging connectivity the risk to AtoN data is relatively low but moving forward, this is likely to change. As technology advances organisations should plan to protect all their data as attackers get more targeted in their approach.



Find out more:

Watch the on-demand webinar "**Cyber Security in AtoN**" where **Jens Ohle, Engineering Manager** at Sealite presented to **IALA Members** on this topic.

Jens' engineering career was launched at Telkom South Africa. Jens also worked as a Team Leader – Systems Integration for a global securities company.

How Does Star2M Work?

The Star2M platform brings all of your assets together into a single hub.

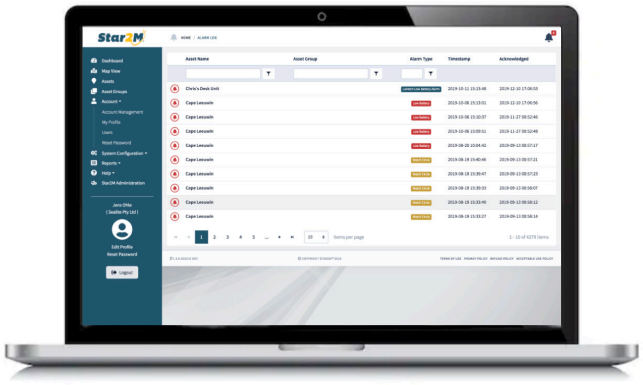
It utilizes military-grade AES-256 encryption in conjunction with high integrity, long term data archives. Star2M works in two ways:

- By IOT and connecting your assets (such as obstruction lights and marine lanterns) digitally to the portal. This allows the user to monitor and control their assets to suit their operational needs.
- By recording asset data and asset conditions directly into the platform via the web portal or mobile App.

This allows the user to perform key tasks such as planning, tracking and scheduling to support optimal asset performance.

The Star2M Portal is available via any internet connected tablet, cell phone or PC. The Star2M Application is also available for iOS and Android smartphone devices.

Operating as a subscription service, Star2M is powered by Iridium®, the Low Earth Orbit Global Satellite service company. It offers pole-to-pole coverage, anywhere, anytime.



Want to Learn More?

For further information on how Star2M can help your business, visit our website at www.star2m.com.

Alternatively, you can contact one of our representatives using the details below.

Head Office
+61 (0)3 5977 6128
sales@star2m.com

Americas
+1 (603) 737 1311
sales@star2m.com

United Kingdom
+44 (0) 1502 588026
sales@star2m.com

Asia
+65 6908 2917
sales@star2m.com