Digitising water access data for regulatory use

DETAILS

SECTOR | Water
STAGE | Strategy and Planning, Project Delivery, Operations and Maintenance
TECHNOLOGIES | Metering, telemetry, analytics

SUMMARY

Typically, the cybersecurity is in the data transfer and collection component. This is where data is sent from the meter via a communications network to be stored either on a server or in the cloud. There are a variety of such transfer networks, such as the well-known phone telecommunication providers, but a variety of private networks are also available. Water authorities or regulators can also build their own networks but this is usually too expensive especially when other providers are available. When selecting a data transfer provider, a thorough understanding of data handling protocols should be developed to ensure data is kept safe and whole. The use of high-level encryptions is important, as is the storage location that data is transferred into. Data should only be allowed to enter or pass through data storage or handling that has the appropriate level of cybersecurity. It is important to ensure that data is not manipulated by the transfer process. The technology is available to ensure that this is the case, but the end-to-end system needs to be packaged together to meet policy and operational needs of water access regulators. The following is a list of typical components and how technology can address the cyber risk:

- Meters measure water volumes – use meters compliant with approved standards
- A local logger collects and stores meter data – use purpose-built loggers with tamper proofing and tamper alerts. Long-term data storage can be an option to have the original data available for comparison.
- A telemetry unit transfers the data via a modem – usually integrated with the logger. Use tamper proof and encryptions as per above and below.
- The telecommunications network carries the data - encryption such as IPsec and VPN
- A data collector to ingest the data – data cleaning without manipulation
- A cloud or server stores the data – use trusted provider or onsite storage

Water access regulation is a complex problem for many reasons. Water is a finite resource usually covering a wide geography such as a river, lake or underground aquifer. There are multiple users and stakeholders that may be using the water for irrigation, industrial purposes such as mining or for drinking water supply. There are also environmental requirements such as “environmental flows” required to let a river maintain its ecological health. The regulation of water access is required to ensure water entitlements are correctly allocated and that allocations are being adhered to. To ensure fair and equitable access of water, and to prevent water theft,
regulators need to be able to measure the amount of water being abstracted and use this data for compliance and enforcement purposes.

The problem being solved by this solution is that existing systems are typically designed for billing purposes and do not provide the required data integrity and data security for purposes of enforcement of the legislation. Furthermore, in many areas, the abstraction of water is not metered correctly and so therefore not providing accurate data. In this case, a regulator cannot ensure compliance to the entitlements. Two important considerations need to be taken into account in the implementation of a secure system for digitising water access data:

- Ensure accurate metering and then provide a system that can transfer the data securely to the regulator.
- Ensure that the data collected is not being “touched” by any other party along the way during which it might be altered. Most data transfer systems, although secure, are about opening up data access and trying to improve integration. This is primarily to improve operational use of the data. The “locking down” of data for use by a regulator is in essence the opposite of this to ensure the data is not altered.

The desired outcome from this use case is data security and data integrity – sufficiently to enable the use of data for compliance and enforcement purposes. For data to be cybersecure, it firstly needs to be safe from other parties and it also needs to reach its destination with all the data accurate and intact.

The continued evolution of cybersecurity measures will always be needed as cyberattacks advance. Technology will need to keep pace to ensure that data is safe. The sovereignty of data, i.e. what country it is held in, is also an area that will likely need some progress. As we seek to collect more data using more global technologies such as low-earth orbit satellites, data is less likely to remain in country. Satellite-based technologies could hopefully address this issue by providing a solution that meets the needs of countries that require data sovereignty.

VALUE CREATED

Improving efficiency and reducing costs:

- Digitising water access data (and associated cybersecurity measures) typically costs more to implement, but overall, an effective and cybersecure system in place will enable regulators to have more confidence in data obtained, meaning less site visits and a reduction in travel costs and time.
- Digitising water access data, as applied to water access regulation, improves the efficiency of obtaining data on water abstraction or water use which may have traditionally been done manually or perhaps without confidence in the data provided digitally. This allows regulators to make more timely decisions and have early warning on any anomalies or breaches to regulations.

Enhancing economic, social and environmental value:

- Digitising water access data ensures fair and legal access for everyone to a valuable natural resource. The effective adoption of such a system will promote economic value by providing stable and foreseen water usage for irrigation and other commercial and industrial uses.
- This provides farmers and business owners confidence in the regulation and allows water users to plan their operations with confidence.
- It also allows regulators to effectively control water abstractions in line with sustainability requirements, helping to promote long-term health of the environment.

Reshaping infrastructure demand and creating new markets:

- As with any regulated process, digitising water access for regulation drives a reshaping of the market’s offering to meet this new demand. This will promote the development of secure and accurate devices to legislative requirements, including water meters, telemetry components, and data receivers and storage solutions.
Demand from regulators will reshape technology development roadmaps to support the regulation. It is expected to create a technology advancement to meet the new markets created.

POLICY TOOLS AND LEVERS

**Legislation and regulation:** Natural resources (water) access regulation requires firm backing in legislation to drive the regulation and enforce change in water usage patterns. Application of cybersecurity standards must be included in legislation to ensure appropriate cybersecurity measures are included in any project development.

**Procurement and contract management:** There are several options for procurement of this digitised system. This can be procured by the regulator or by another part of government, or it can be procured by the water user in a ‘user pays’ system. Specifying the technology to be used can be determined through a competitive procurement process or a performance specification can be used to allow an open market to find solutions. In a user-pays system, water users will be required to make their own decisions in terms of the purchase and installation of the components. Government would use inspection and verification as tools to ensure compliance.

**Funding and financing:** Governments can choose to fund the digitisation or choose a ‘user pays’ systems. Where the system is not fully funded by a government, some government expenditure can be used to support certain elements of the project. For example, funding can be provided to promote technology development to meet the cybersecurity needs of state or national water access regulation. Funding can also be provided for testing of devices and protocols to ensure devices and data transfer is safe and secure.

**Effective institutions:** Natural resources access is better regulated through the use of effective institutions to help support the enforcement of legislation. Institutions such as industry bodies or associations can provide training to ensure qualified personnel are available for cybersecurity deployment, device management or installation. Institutions can be also be set up to carry out compliance checking. Cybersecurity depends as physical aspects such as vandal-proof installations and correct procedures are followed. Institutions can be used to ensure this aspect is well understood and enabled. National and international standards organisations e.g. ISO, can be used to maintain quality requirements. More specifically, standards and procedures can be used to set what protocols are to be followed when for example when a data breach occurs.

**Transition of workforce capabilities:** A small but dedicated workforce is needed for natural resources access regulation. Key skills are in-field meter and device management, telecommunications, meter data management and visualisation. Ensuring data accuracy and integrity also requires cybersecurity to be applied to the above elements so workforce capabilities need to include this.
IMPLEMENTATION

Ease of Implementation

The challenge for implementing digitised water access data with cybersecurity in this context is the extra effort required above typical operating parameters. Water users and industry partners may need consultation and education to understand the requirements and specifications for such an implementation.

Cost

Telecommunications typically operate in a competitive market so costs are not prohibitive. It is perhaps more important to ensure the provider has the right geographic coverage and actually has effective cybersecurity in place.

Country Readiness

Digitising water access with cybersecurity can be applied anywhere given the in-field devices are robust, telecommunications are in place and cloud services are available. The regional maturity of local telemetry and telecommunications providers and their approach to cybersecurity is the aspect limiting deployment across regions.

Technological Maturity

Digital systems for water access are fully mature and can be implemented now, pending compliance with regional data and cybersecurity standards. As telemetry and telecommunications technologies develop (e.g. 3G to LPWAN) it is important to ensure that new technologies retain the cybersecurity element of previous technologies.

RISKS AND MITIGATIONS

Safety and (Cyber)security risk

Risk: Cybersecurity always brings the risk of the unknown until it is tested.

Mitigation: Rigorous testing at all phases is required. Use protocols and encryptions that are known to be effective for cybersecurity.

Risk: To ensure data security and data integrity, the whole data transmission chain must be secure. “A chain is only as strong as the weakest link” applies here.

Mitigation: Ensure the same level of security is applied to every element in the transmission chain from meter to cloud.

Risk: In-field devices for capturing data are an access point to tamper with data.

Mitigation: Tamper-proof devices must be used with an appropriate level of vandal proofing. Tamper alerts and logs should be incorporated for any cables that are cut or doors that are opened. Access to the data logger must be password protected.

Risk: Interception of data transfer by a “stingray”

Mitigation: Have procedures in place to check when data is expected to be received and actions for when it is not.

Risk: Transfer of data is not secure
Mitigation: Ensure all connections are authenticated and encryption protocols are in place.

Risk: Data from another source is sent to the data collector/ingestor.

Mitigation: Ensure access to data collector/ingestor is authenticated prior to transfer from the logger.

Risk: Environmental factors can play a large part in causing loss of data. It is not just the “hacker” that is of concern as insects, heat, moisture and exposure can damage equipment.

Mitigation: All in-field devices should be manufactured to suit the environment they are to be deployed in.

Risk: Cloud Storage is accessed by 3rd parties.

Mitigation: Ensure cloud storage is encrypted.

EXAMPLES

<table>
<thead>
<tr>
<th>Example</th>
<th>Implementation</th>
<th>Cost</th>
<th>Timeframe</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSW Dept of Planning Industry and Environment</td>
<td>Digitisation of approximately 8000 water abstraction points are planned for completion in 2021 to assist with enforcement of water allocations. Devices and components have been developed and are currently in field testing.</td>
<td>Cybersecurity requirements would expect an increase in vendor costs but the reshaping of the market from the regulatory driver, coupled with a free market procurement process, leads to telemetry devices being available at normal market prices ranging from A$500-$2500 per end point.</td>
<td>The timeframe to implementation is approximately 6 months due to two elements: custom build of a secure data receiving portal and time for the market to respond with development of new devices to meet the cybersecurity requirements.</td>
</tr>
</tbody>
</table>