DATA SECURITY – THE CHALLENGE IS OFTEN BIGGER THAN YOU THINK

Meters have long been construed as cash registers for utilities. As such, the accuracy and authenticity of data used for billing has always been of concern to them, says Kaushik Ghosh, Group CTO, Secure Meters.

As smart metering becomes more prevalent and the desire to maximise operations and efficiency driven by data increases, data security is becoming a matter of significant concern to utilities, customers and society at large. Never before has the threat of remote connectivity, control and ability to disconnect supply been perceived at such humongous proportions. So much so that in view of the potential vulnerabilities that could be exploited through remotely connected smart meters, the UK Government has declared the smart metering system as Critical National Infrastructure and brought it under the purview of the National Cyber Security Centre.

Remote disconnect of a multitude of meters can destabilise the grid and potentially lead to blackouts. One of the lesser known potential threats for a utility is known as a masked remote disconnect. This is a breach along any element of the data value chain – for example, a future-dated tariff could be maliciously updated and impact the tariff cost to such an extent that a multitude of prepaid meters simultaneously and automatically disconnect, leading to customer service chaos and causing the grid to falter.

Problems in the end-to-end data chain can affect billing information and accuracy, which may have a severe impact on a utility's reputation, regardless of where the inaccuracy occurred. Along each node of this value chain, there are vulnerabilities, and these determine the risk landscape that needs to be protected. Developing strategies to protect this landscape has to take each one of these nodes into account.

Besides the utility and public at large, the need to protect the interests of the end consumer must not be undermined. As a service provider, a utility has an obligation to ensure that the end consumer is receiving a service that is appropriate to their needs. This is only possible if the data used for billing, for instance, remains authentic and accurate through the entire data chain of metering, reading, data processing, billing and payment collection.

With the increase of data availability and data gathering, consumers are becoming ever mindful of the need for privacy and the assurance that their data will be protected. Data privacy is becoming more and more relevant as the levels of data generated increases, and there are both legislative and regulatory moves to safeguard consumer information such as consumption profiles, disconnect status, alerts, accounts and debts.

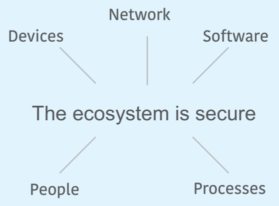
Smart meters also pose risk to vulnerable customers such that 'electrically assisted' consumers may be disconnected by a breach of security regimes. Also, automatic remote reconnection of supplies (electricity or gas) may lead to safety risks for unaware consumers.

Data security strategies

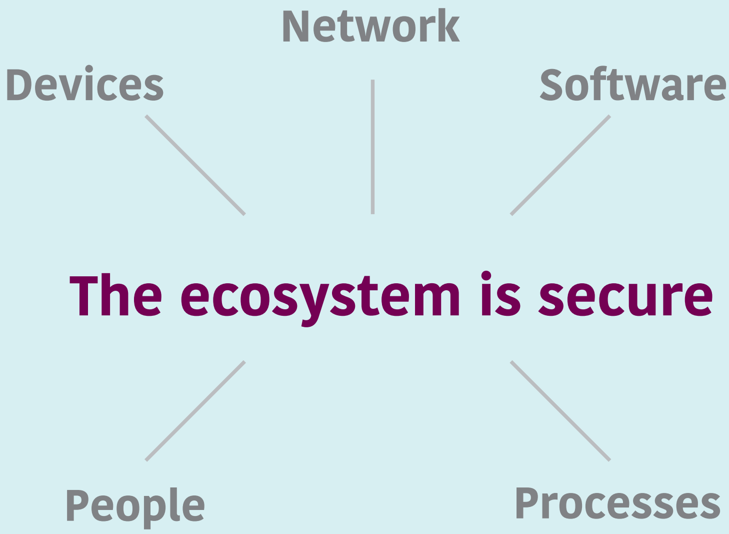
Security is not a one-off implementation; it is a continually evolving application and an element of all modern businesses. To develop a data security strategy, a clear picture needs to be formed of the devices, the network, the systems deployed and the people and processes in the ecosystem. By understanding what the risk exposure is, an organisation can put a suitable mitigation strategy in place. Security considerations include:

Data protection

> "Clear picture needs to be formed of the devices, the network, the systems deployed and the people and processes in the ecosystem."



SECURE



Network

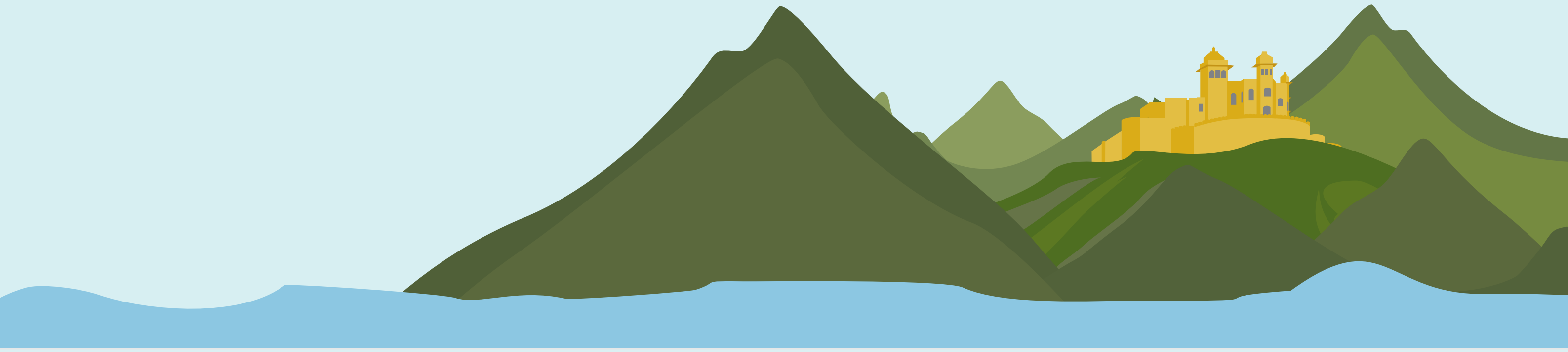
Devices

Software

The ecosystem is secure

People

Processes



Single element security will fail

www.securemeters.com

Devices: Are there any bugs or weaknesses that can potentially be exploited? Are there any gaps in the device security? Is your metering supply chain assessed for its security practices?

Network: What are the potential vulnerabilities along the entire communication network? What is the exposure to phishing, eavesdropping, spoofing or distributed denial of service attacks, and what are their potential impacts?

Systems: System vulnerabilities include malware, ransomware, data breaches or access breaches, which may affect data integrity and accuracy. How well protected are the systems?

People and processes: How easily could staff members by socially engineered? Are there disgruntled employees that may be a threat? Is adequate time spent on training staff about security issues?

There are a number of existing strategies already available for guidance, such as the American National Institute of Standards (NIST) Smart Grid security or ISO/IEC 27001:2005 ISMS framework.

Three-layer IT architecture

Often smart meter security is merely perceived to consist of a few sections in the meter and software buying-specifications, which are checked for compliance during the buying process and then forgotten. In reality, end devices only form a small element of the entire vulnerability landscape that demands continuous protection. A robust cyber security strategy must be formulated across the enterprise and governed from the CEO's desk. A three layered architecture has been proposed to help conceptualise the complete landscape.

Technology

Working from the bottom up and starting with the technology layer: consideration needs to be given to the level of encryption and security implemented in 'end point devices,' such as meters and other networked assets like gateways and data stores. This encompasses anything within this ecosystem from meters to computers, and also covers network, host and content security, along with verification of the integrity of both the data and the data location.

Additional considerations are the security of data in storage and the security of data in transit. When data has been stored, clear parameters need to be stated which determine who has access to the information, that the information is sufficiently protected and that there are active audit trails and procedures in place. Instances of wilful tampering with the billing data are not uncommon.

The utilisation of public/private keys, their distribution, the security of the certification authority, and managing crypto tokens and keys are also very important considerations in the security strategy. Often all meters are left with the same keys, or where unique keys are deployed, the key management and distribution is weak and gives a false sense of security.

People and processes

Technology and governance are essential, but if security concerning people and processes is not in place, technology and governance will not bridge the gaps. The entire value chain of service development, data management, security procedures, incidence management and prevention are critical to success.

Failure to follow procedure, human error, ignorance or a malicious attack can all ultimately have the same result – increased vulnerability of data and potential liability for the utility.

The people element of any security strategy starts with appropriate training and education about security practices. It is essential to train, prevent and protect across all aspects of the business.

In many cases, the people elements of security are likely to be the most vulnerable due to the perception that security gets in the way of speed, is counterintuitive, or doesn't take operational requirements into account. As a result, a security mindset needs to be a priority across the entire organisation.

Security is no longer a bolt-on option. It needs to be part of the design right from the beginning of the development of a new product and/or service offering. Data backup, recovery and retention policies need to be developed on top of any legal or regulatory requirements. Routine security updates and patches need to be applied based on a judicious assessment of needs.

Important is the development of standard operating procedures if a data breach has occurred, detailing who needs to be informed, how the potential fallout is assessed and what recovery efforts need to be undertaken. However due to the fragmented nature of legal, regulatory and security frameworks across an organisation, very often there is not a single unified approach or point of contact of sufficient seniority to ensure compliance and effective implementation. The concept of end-to-end governance should be built into the architecture.

Across all levels of the security architecture supply-chain management and security, as well as supply-chain vetting needs to be documented and assessed and reassessed regularly.

Security is effectively a consideration across an entire company, from HR to procurement, from IT to operations. Social engineering is becoming increasingly sophisticated, and training and awareness around current and emerging social engineering methods will need to be shared, and policies should be in place to reduce the risk.

Governance

Security governance, the top part of the three-layer architecture, needs to be driven from the top down within any organisation. It must have the attention of the topmost table within the organisation in order to bridge company silos and functional departments.

Governance encompasses development of a security policy, assessing risk profiles, developing a security strategy and controlling through audits and compliance.

Risk management entails examining the potential for exposure across the entire landscape and within this threat canvas, determining the risk probability and the risk impact across each element – devices, network, systems and people and processes.

Considerations include:

- What is the probability that somebody can hack into the network and disconnect multiple devices?
- What is the probability that somebody can change the billing data?
- The motivation behind a potential intrusion – is it terrorism, organised crime, financially motivated or potentially disgruntled employees?

Once the probability of each of these risks has been identified, the impact of that risk needs to be assessed. For instance, will it impact a single meter only, or is it likely to affect the entire population of meters? Is it likely to have a more significant impact on the broader national grid?

The risk profile analysis will determine the organisation's security strategy at a governance level and will define appropriate audit systems to monitor compliance with both regulatory and internal governance structures.

While much of the three-layer security approach is common-sense, the implementation in an effective end-to-end manner is still something of a challenge. Many technology solutions can be implemented to enhance security, but unless awareness and accountability for security reaches the top table in the organisation, results will be mixed. SEI