CSC

50 YEARS STRONG

IDENTIFYING INHERENT SECURITY RISKS

Advanced Metering Infrastructure and Smart Meters

Introduction

Advanced Metering Infrastructure (AMI) and Smart Meter technologies offer utilities opportunities to enhance customer service and improve their operational efficiency. AMI enables utilities to measure consumption in real time and use this data to promote energy efficiency, demand response and time-based pricing options. It also automates the collection of meter data, enables remote management of meters, detects outages and theft, and improves field, billing and call center efficiency. AMI is also being used to extend advanced energy use technology (such as smart appliances) into customers' premises.

These opportunities also pose challenges for utilities, increasing inherent security risks. System reliability, consumer privacy, network integrity, interconnectivity and the integration with critical back office applications are far more vulnerable now than with traditional metering systems. With proper planning and strategy, these risks can be effectively mitigated to an acceptable level. In our experience, utilities should consider the following security risks at the onset and during an AMI program deployment:

- Vendor and product selection
- AMI network management and system integration
- Corporate governance and regulatory compliance
- Privacy and integrity of data
- Identity and access management
- Physical, operational control, and infrastructure security assessments and remediation
- Web services and portals
- Business continuity and resiliency
- Security events and network monitoring (7x24x365)
- Digital investigative (forensics) assessments
- Vulnerability and threat management

AMI Security Risks

AMI is a vast, complex and highly integrated network of multiple systems and technologies. AMI security risks are segregated and highlighted in five functional areas:

1. **Meters:** Devices that measure usage at a customer premise. Meters also serve to delineate the home area network from the rest of the AMI. The primary threat facing meters is that of physical tampering. AMI technology increases the risk of BOBA (Break One, Break All) threats that could compromise every meter in the network. AMI meters allow an additional level of physical security by providing real-time alerts if a meter case is opened. In addition, the advanced circuitry of an AMI meter allows the meter to detect more subtle attempts at tampering, such as reversing or switching the polarity of the electrical phases, magnetic anomalies or tampering with internal clock settings. As with any device, an attack or even a routine operational issue may cause a failure in the meter. It is imperative that

meters and other field-deployed hardware automatically fail to a "safe" condition. A failed or disabled meter must be able to maintain tamper alerting/evident capabilities, and if possible, continue to record use. A meter's ability to respond to security, mechanical or logical faults and maintain adequate security controls is a key consideration for selecting the right AMI technology.

2. Home Area Network (HAN): Network of devices on the customer's premise, such as smart appliances and power management devices, interfacing directly with the utility. HAN poses risks to AMI particularly as user-installed devices interface with the utility's AMI network. Assuring the authenticity of these devices and the integrity of the data they provide are a key consideration for mitigating the risks posed by HAN. Existing standards for building HAN such as ZigBee SE provide a centralized certifying authority for devices and establish a local authenticating authority to maintain the trust network during normal operations.
3. Local or Neighborhood Area Network (LAN or NAN): Provides local connectivity from the meter to the backhaul network. The network between endpoints (meters) and access points (LAN or NAN) can span a large geographic area and may cause a malicious user to intercept or interrupt data transmission. An open, un-segmented network could increase the risks of security breach or fault to propagate across the entire AMI network, exposing data and limiting functionality. Worst case, a utility may be vulnerable to the loss of control of their network to a dedicated attacker.
4. Wide Area Network (WAN): Provides connectivity from local (neighborhood) networks to the network management system. This may not be necessary depending on the technology used for the LAN. Transporting data from local access points to the centralized back office poses a large threat to utilities as it concentrates on a large volume of user data. In addition, any availability issues with the backhaul network could have a very significant impact, as a single access point may be responsible for transmitting data from tens of thousands of endpoints. Backhaul networks are often secured by building a secure tunnel across public, multiple redundant networks such as existing 3G networks, frame relay networks, or the Internet. Access points can be made redundant either on a point-by-point basis or through the use of overlapping areas served by different access points.
5. Network Management System (NMS): Back-end systems that provide monitoring and management capabilities for utilities. NMS allows utilities the ability to manage meters and endpoints from a central location. Since NMS users have access to extremely sensitive AMI data and functionality, it is imperative to impose proper creation of user roles, strong user management, and strict audit and monitoring practices for operations. The nature of AMI also requires strong governance and effective enterprise-wide business continuity planning and disaster recovery programs. Since critical infrastructure cannot tolerate a single point of failure, redundant operational capability must be a component to the NMS.

Protected Enterprise

- Links boardroom strategy to operations and IT policy
- Balances cost with value-at-risk, providing the most cost-efficient solution to delivering the protection that you need
- Creates a flexible compliance framework and governance model and makes it part of daily business operations
- Increases visibility of critical assets, processes and data and focuses spending on protecting what matters
- Builds trust with partners, suppliers, customers, regulators and shareholders

CSC AMI Security Services

Today's utilities face orchestrated, intelligent threats that must be handled by an integrated and fully coordinated security approach, extending throughout and across the business enterprise. Compliance with existing, new and evolving regulations and standards is an adaptive, iterative process, thoroughly ingrained into daily business operations. Proper assessment practices and tools and effective mitigation of security risks must be considered at the very earliest stages and during the deployment of an AMI program. This is especially important when selecting equipment such as meters and HAN devices.

As one of the largest, global Business and IT services providers in the world today, our Security Services are core to our own operations as well as those of our Utility, Chemicals, Public and Commercial sector clients. We provide a variety of security services for major energy and utility companies in North America, Europe, Australia, and public sector clients including the Department of Energy's Strategic Petroleum Reserve.

BUSINESS SOLUTIONS
TECHNOLOGY
OUTSOURCING

Our Protected Enterprise solution is a complete suite of risk and security services to assess and protect the enterprise. It offers an innovative yet practical approach, taking a business-focused view and balancing risks and protection to create true business value. Combining the business expertise of our information risk managers, utility and public sector expertise with an extensive set of technical capabilities across a wide range of systems and platforms, our Protected Enterprise solution delivers a cohesive enterprise-wide security program. Our global Security Solutions practice comprises over 1,200 security professionals with a wide range and depth of skill sets across every major industry segment as well as U.S. federal agencies and state and local government.

In addition to maintaining a leading Security Center of Excellence, we maintain a variety of security labs in all major regions and our solutions span the entire lifecycle of security services — assess, plan, build, manage and support. We manage Security Operations Centers in North America, Europe, Australia and India. We are a recognized leader and innovator in areas such as computer forensic services and biometric engineering services. We manage some of the most critical strategic facilities including the U.S. Department of Defense (DoD) Cyber Investigation Training Academy and the DoD Biometrics Fusion Center.

Summary

With proper identification and assessment of risks, and the design of controls and mitigation strategies throughout the AMI deployment process, the security risks associated with your AMI program can be reduced to an acceptable level, and the benefits of improved customer service and operational efficiency can be realized. For more information, please contact:

Denise Antoniadis
Partner and Utility Industry Lead
kantoniadis@csc.com
707. 529.9325

About CSC

The mission of CSC is to be a global leader in providing technology enabled business solutions and services.

With the broadest range of capabilities, CSC offers clients the solutions they need to manage complexity, focus on core businesses, collaborate with partners and clients, and improve operations.

CSC makes a special point of understanding its clients and provides experts with real-world experience to work with them. CSC is vendor-independent, delivering solutions that best meet each client's unique requirements.

For 50 years, clients in industries and governments worldwide have trusted CSC with their business process and information systems outsourcing, systems integration and consulting needs.

The company trades on the New York Stock Exchange under the symbol "CSC."

CSC
266 Second Avenue
Waltham, Massachusetts 02451
United States
+1.800.272.0018
www.csc.com

Copyright © 2009 Computer Sciences Corporation. All rights reserved.

DS09_0340