



TESCO METERING



925 Canal Street, Bristo, PA 19007

215.228.0500

Tescometering.com

## Protecting the Grid: Securing Meter Data and Systems in the Age of Cyber Threats

### Overview

Utilities are under increasing pressure to safeguard their systems and data. As critical infrastructure providers, they are prime targets for cyberattacks ranging from ransomware to data manipulation. For utility leaders, cybersecurity is not just about protecting IT—it is about defending customer trust, ensuring operational continuity, and meeting compliance obligations.

This paper explores the rising cybersecurity threats facing utilities, the risks of fragmented meter data systems, and the serious consequences that can result from an attack. It then outlines best practices for building resilience and highlights how solutions like **TESCO's Meter Manager Software** help utilities strengthen security without slowing operations.

### The Cybersecurity Landscape for Utilities

Utilities today are increasingly viewed as high-value targets by cybercriminals. A successful attack on a utility company has the potential to disrupt services for thousands—or even millions—of people, making these organizations especially attractive to bad actors.

At the same time, the types of threats utilities face are growing more sophisticated. No longer limited to basic viruses, utilities must now contend with ransomware, insider threats, and data manipulation schemes designed to erode trust in billing and operational data.

Adding to this challenge is a tightening regulatory environment. Standards such as **NERC CIP**, along with oversight from state commissions and federal guidelines, increasingly require utilities to implement secure and auditable systems. Cybersecurity is no longer a back-office IT concern—it is a core responsibility tied to compliance, operational integrity, and customer confidence.

## Vulnerabilities in Meter Data Management

Despite the growing risk, many utilities still manage meter data with fragmented and outdated methods. Spreadsheets and siloed databases remain common, yet they are highly vulnerable to unauthorized access and tampering. Paper logs and manual processes compound the problem, creating records that can be lost, altered, or left incomplete. Even when digital systems are in place, gaps between AMI, billing, and enterprise platforms create blind spots that attackers could exploit.

These vulnerabilities extend far beyond billing data. Modern **Advanced Metering Infrastructure (AMI)** systems often include **Remote Connect/Disconnect (RCDC)** switches that allow utilities to remotely enable or disable electric service without a field visit. While this capability improves efficiency and safety, it also introduces a critical control point that must be protected.

If an attacker gains access to the communication path, meter head-end, or associated control systems, they could issue unauthorized disconnect or reconnect commands—potentially affecting thousands of customers simultaneously. Research sponsored by the U.S. Department of Energy and the University of Illinois has shown that **mass disconnection or reconnection events**, even affecting **less than 2% of system load**, could destabilize portions of the grid if executed in a coordinated attack. Unauthorized RCDC operations could also be used to falsify outage conditions, delay restoration, or cause load oscillations that compromise grid stability.

The exposure does not stop at the meter. Because AMI, **asset management**, and **Customer Information Systems (CIS)** are often interconnected, a breach in one can serve as a gateway into others. The asset management system—which tracks meter configurations, firmware versions, and connectivity status—may inadvertently provide a pivot point into operational or enterprise networks. Through these links, attackers could alter device configurations, disable tamper alarms, or access sensitive customer information.

A compromised CIS, in particular, poses significant risk because it houses **Personally Identifiable Information (PII)** such as customer names, addresses, account numbers, and in some cases Social Security numbers. Exposure of this data can lead to identity theft, financial fraud, and legal or regulatory penalties.

Additionally, outage and load data flowing through AMI systems are essential for grid monitoring, forecasting, and restoration. Manipulated or falsified data could cause dispatch errors, mislead outage management systems, or hinder emergency response. In short, vulnerabilities in meter data management are not theoretical—they represent **real and multifaceted openings** in a utility's cyber defenses.

## What's at Stake if an Attack Occurs

The consequences of a cyberattack on utility systems or meter data can be severe and far-reaching.

### Financial Impact:

Utilities risk losing millions of dollars in unbilled usage if meter data is corrupted. Ransomware demands and system recovery costs can escalate quickly, while billing errors caused by tampered records may lead to refunds or settlements. Unauthorized RCDC events can cause physical service interruptions that require expensive field verification and reconnection efforts.

### Regulatory and Legal Exposure:

Noncompliance with cybersecurity or data protection rules can result in significant fines. Regulators may impose mandatory remediation orders requiring costly overhauls of systems and processes. In addition, a data breach exposing PII from the CIS could trigger privacy violations and class-action lawsuits.

### Operational Disruption:

Manipulated or inaccessible data can interfere with time-of-use billing, outage management, load forecasting, and restoration efforts. In extreme cases, compromised AMI or RCDC controls could disrupt grid stability or delay emergency recovery. Recovering from such incidents often diverts staff for months, hindering progress on critical projects.

### Reputational Damage:

A utility that experiences a cybersecurity breach risks losing customer trust, drawing negative media coverage, and facing increased scrutiny from regulators and stakeholders. In an industry built on reliability and public confidence, reputational harm can be as devastating as financial loss.

## Building a Secure and Compliant Foundation

The good news is that utilities can mitigate these risks by adopting best practices that emphasize both **compliance and resilience**. Centralizing meter data into secure, purpose-built platforms eliminates vulnerabilities created by spreadsheets and disconnected databases.

Solutions like **TESCO's Meter Manager Software** provide a trusted system of record—offering both traceability and protection. Role-based access controls limit sensitive functions, including RCDC operations, to authorized personnel only. Encryption and secure APIs safeguard data both at rest and in motion, maintaining synchronization across AMI, billing, and enterprise systems.

TESCO's software also supports **audit-ready reporting**, generating consistent, verifiable documentation to meet regulatory requirements. In the event of a cybersecurity review or audit, utilities can demonstrate adherence to NERC CIP and state cybersecurity mandates with ease.

However, technology alone is not enough. **Employee awareness and training** remain vital. Personnel who understand cybersecurity principles, data classification, and secure workflows play a critical role in preventing accidental breaches and insider threats. Regular exercises, password hygiene, and simulated phishing awareness campaigns strengthen this first line of defense.

To further harden RCDC operations, utilities should:

- Require **multi-factor authentication** for remote switch controls.
- Implement **command logging and real-time alerts** for RCDC events.
- Introduce **rate limiting or randomized delays** to prevent mass disconnect attacks.
- Isolate RCDC command channels from general AMI traffic through **network segmentation**.

These measures align with DOE-recommended AMI security practices and help utilities ensure both system integrity and customer safety.

## From Risk to Resilience: A Practical Example

Consider a regional utility that relied heavily on spreadsheets and paper logs to track its meter population. Audit preparation was burdensome, and leadership was increasingly concerned about cyber risks. After adopting a secure, centralized platform for meter data, the utility transformed its operations:

- Unauthorized access was curtailed through user-based permissions.
- Compliance reporting was automated and streamlined.
- RCDC command execution was restricted to verified personnel and fully logged.
- Audit preparation time was cut dramatically, saving staff hundreds of hours annually.

Most importantly, executives gained confidence that their meter data was **accurate, traceable, and protected**. Utilities using **TESCO's Meter Manager Software** are seeing

similar results—turning potential vulnerabilities into strengths and building long-term resilience against evolving cyber threats.

## Conclusion

Cybersecurity is one of the most pressing challenges facing utilities today. While the threats are serious, they are not insurmountable. By consolidating data, securing control systems, and embracing best practices, utilities can protect themselves against financial losses, regulatory penalties, operational disruptions, and reputational damage.

**TESCO's Meter Manager Software** provides utilities with a proven framework for defense. With features ensuring data integrity, secure RDC management, audit readiness, and encrypted integrations, Meter Manager helps utilities not only comply with regulatory requirements but also build resilience and customer trust in an increasingly complex world.



TESCO METERING