Mission Critical: The Cybersecurity Struggle for Utilities

DATA PRIVACY SOLUTIONS | FEB 26, 2015

Seemingly not a day goes by without reports of another company penetrated by a cyber attack. And, with each hack, another weakness is exposed in the armor protecting customer information in banks, retailers, and health insurers. Utilities are no exception. Analysts, public utility commissioners, elected state and federal officials, and utility executives are all paying attention to cybersecurity with ever greater focus.

While the issue of cyber security is one that utilities and regulators seemingly prefer to discuss behind closed doors, investors, analysts and regulatory agencies are engaged on the issue. The Federal Energy Regulatory Commission, North American Electric Reliability Corp. (“NERC”), and state regulatory commissions are all focusing on utility best practices, protection of both the grid and customer information, and ensuring that exposures are minimized and potential intrusions are mitigated as quickly and with the least disruption possible.

At the recent cyber summit at Stanford University, President Obama announced an Executive Order that is designed to ensure greater information sharing between the private sector and the government. Pursuant to that Executive Order, the Department of Homeland Security is responsible for collection and distribution of information. While information sharing is crucial, the need for timely, actionable information is most important. Companies and state commissions are developing expertise and securing adequate security clearance to receive that timely, actionable information. More needs to be done to ensure this evolving threat continues to receive the appropriate attention.

An example of regulators engaging on cyber issues includes commissioners and staff of several states in the PJM region voluntarily working together with FERC to minimize redundancy between state and federal cyber regulation applicable to utilities. This group shares information and acts as a conduit for information from FERC to state commissions. This is a good start, but clearly is not the ultimate resolution of the regulatory issues in the cyber area of utilities.

In a recent conversation, one Wall St. firm that covers the utility industry estimates the annual cyber security spend at $1 billion. These expenses are typical in that they are necessary expenses to ensure deliverability of power to customers. And, these expenses will be paid for by ratepayers as the evolving cyber threat is now a part of the ordinary course of business for utilities of all sizes. By their very nature these expenses are also subject to a prudency review by the appropriate regulators. This necessitates that state commissions develop expertise in the field of cybersecurity both for understanding of the cyber risks as well as identification of appropriate expenses, such as avoiding gold plated systems that increase rate base but are unnecessarily expensive.

The protection of the utility infrastructure from both cyber and physical attacks is crucial. The work on cyber issues is under way at federal and state regulatory agencies. The Obama Administration’s attention to this issue and the desire to ensure information is shared is a good step. Even with that, more work will need to be done. The cyber defense playing field is constantly changing.