Cybersecurity Is a Priority— But Where Do You Start?

By Doug Westlund

Cybersecurity continues to escalate as a critical issue for utilities of all sizes. Yet utility leaders often feel overwhelmed by how to begin developing and implementing an appropriate cybersecurity program.

Municipal utility general managers, governing board members and other senior officials must ensure that all staff and community stakeholders treat cybersecurity as an essential component of reliability, revenue assurance and risk mitigation. This clarity of purpose will enable the utility to establish specific roles in cybersecurity among the various utility and city departments. It also sets the right organizational tone for IT and operations departments who need to cooperate more than ever as traditional responsibility boundaries increasingly overlap. Most importantly, this senior-level attention should be directed toward a specific process for identifying vulnerable assets, developing a cybersecurity plan and implementing a cybersecurity program that can be integrated into the utility's governance process.

Expanded use of digital technology combined with increased interconnectivity among generation, transmission and distribution systems has made the grid less secure. For example, the reach of SCADA systems is expanding to substations and other remote locations, opening up more avenues for hackers or terrorists to exploit. But utilities have been slow to address this increased risk, often due to budget concerns and cultural resistance at the staff level.

At a typical utility, the IT department focuses on "virtual" assets, including computers and servers that contain customer usage data and billing information. Engineers and other operational departments focus on maintaining the physical assets of the generation, transmission and distribution systems. However, as utility technology systems increasingly involve integrated software and Web-based solutions, the operation and management of these physical unsecured assets is moving to virtual systems often under the responsibility of the IT group. The gap between the functions and priorities of the IT and operations groups at electric utilities is capturing the attentions of hackers and other bad actors.

As remotely deployed field devices and SCADA systems are increasingly brought into the IT environment, they open up new points of attack or "threat vectors" for hackers. These new threat vectors are especially vulnerable for three reasons.

Legacy technology. Unlike IT systems that are constantly and often automatically updated with service packs, new releases and bug fixes, operations technology devices are frequently running the same software they used when initially installed, which in many cases can be 10-15 years old or older. Moreover, these devices have virtually no security capabilities because they were installed at a time when an "air gap" or a physical separation from IT systems was considered "secure."

More sophisticated hacker tools. Hackers are developing tools and techniques at an alarming rate.

Accountability gaps. The rigid silos between IT and operations departments may be the most significant area of vulnerability for utilities.

The solution is for senior management to make sure cybersecurity becomes an integral part of the IT-operations convergence conversation, as the utility leadership establishes clearly defined and coordinated roles and responsibilities. All of this is not as daunting as it may seem. On their own or in coordination with their joint action agency, utility leaders can build an effective cybersecurity program.

An effective cybersecurity solution provides a public power utility with operational, financial and regulatory compliance benefits but only if the solution is a priority for the utility leadership, as well as comprehensive, affordable and easy-to-use. If cybersecurity is treated as an afterthought, the chances of success are much lower. ∎

Doug Westlund is chief executive officer of N-Dimension Solutions Inc., provider of cybersecurity solutions in affiliation with Hometown Connections.

Advertisers Index