ITC Holdings Focuses on Protecting Its Physical and Cyber Assets

By Andy Hilverda

Vandalism, theft, and the potential for sabotage or acts of terrorism have motivated the electric generation and transmission industry to seek viable security solutions. In doing so, they face unique challenges because of the way the industry is structured. Companies must secure their facilities and protect their physical and electronic assets while managing access to their properties state-to-state over geographically widespread regions.

ITC Holdings, Inc. has taken extraordinary steps to protect their physical and cyber assets in order to maintain the integrity of their bulk electric system. Headquartered in Novi, Michigan, ITC builds, maintains, and operates 15,000 circuit miles of overhead and underground transmission lines that carry electric power to more than 13 million people, serving an area of nearly 80,000 square miles.

Recognizing the serious impact to the local and national economy and to people's lives when the power goes off, ITC makes it a priority to protect the transmission grid and provide efficient, reliable energy to its customers. ITC's vision is to have highly effective processes and procedures in place that meet and exceed the new government security standards.

Robert Blickensdorf, ITC Security Manager, is responsible for project management as it relates to the installation, maintenance, and operation of physical security at ITC facilities. He serves as the liaison between ITC and local law enforcement and other security organizations within the industry.

Blickensdorf says, "ITC corporate leaders realize the importance of protecting our physical and electronic assets and have been very supportive of our security initiatives." Facing an overwhelming array of choices and costs, ITC developed a risk-based methodology for pursuing a balanced approach to accomplishing their security goals. ITC had to determine the type of physical security that would best serve each particular location, install and integrate the necessary security devices, and then maintain and monitor the effectiveness of the system.

Facing threats of vandalism and theft due to the high price of copper and other metals on the open market, ITC adopted measures to prevent someone from accessing one of their sites with the intent of stealing metal and, in the process, causing damage that affects the reliability of the system or the safety of employees and contractors. Vulnerability is heightened at ITC's remote sites because of their isolation. In an effort to address these concerns, they installed security equipment to prevent vandalism or theft at these sites.

ITC Headquarters (Photo provided by Robert Blickensdorf at ITC)

Blickensdorf says, "We do not want to give any individual or organization the opportunity to sabotage the system because the impact is too far-reaching."

Live camera mounted on a pole by perimeter fence. (Photo provided by Robert Blickensdorf at ITC)

Blickensdorf oversees the operations of ITC's Security Command Center which is staffed with personnel, 24 hours per day, 7 days per week. The Security Command Center monitors live cameras and alarm systems throughout their sites. Video verified intrusion alarms have become more practical as the costs of CCTV (closed circuit television cameras) have been declining, making it a capable solution for enhancing their security.

To date, ITC has installed at least 300 live cameras along with an integrated alarm system at 30 of their sites. With their sophisticated security system in place, Security Command Center personnel can quickly determine whether an intrusion is non-threatening or something more serious.

ITC's physical security projects encompass ITC headquarters, substations, and warehouses. In addition to the live cameras and alarm system, they have installed perimeter fence intrusion monitors, photobeam towers, infrared illumination devices, motion detection towers, and other physical security equipment at strategic locations. They also have an integrated online access card system installed throughout their facilities. If there is any unauthorized access or other alarm, this information is quickly transmitted to the Security Command Center for action.

The Federal Energy Regulatory Commission (FERC) and the North American Elec-

Reprinted with revisions to format, from the April 2009 edition of **UTILITY PRODUCTS**

CyberLock Padlock on an ITU Cabinet (Photo provided by Robert Blickensdorf at ITC)

tric Reliability Corporation (NERC) have established enforceable security standards to prevent electronic and physical attacks that could cripple the energy industry which is a critical part of our nation's infrastructure.

In January, 2008, Critical Infrastructure Protection (CIP) Reliability Standards were approved for the purpose of protecting the physical security of critical cyber assets. CIP Standard 006-1 "requires a responsible entity to create and maintain a physical security plan that ensures that all cyber assets within an electronic security perimeter also reside within an identified physical security perimeter. The physical security plan . . . must contain processes for identifying, controlling, and monitoring all access points and authorization requests. The Reliability Standard also requires that the logging of physical access must occur at all times, and the information logged must be sufficient to uniquely identify individuals."[1]

There were logistic challenges that confronted ITC in developing a strategy for meeting the CIP Reliability Standards. As they began to tackle these issues, they looked for a secure access control system that would provide the flexibility they needed. Most importantly, they needed a system that could bring key control and an audit trail to their remote sites without requiring power at the lock.

Blickensdorf comments, "We required a system that could eliminate the risks associated with the duplication of keys, and assist us with CIP compliance by tracking contractors and employees that go into locations that contain critical cyber assets." They were looking for a product that could be integrated with the sophisticated security equipment and systems they already had in place.

After thorough research, the organization chose to implement CyberLock and proceeded to integrate the electronic lock system into their existing systems. ITC solicited the help of Janna Access LLC, an access control integration company located in Columbia Station, Ohio. "Janna Access came on site and worked very closely with our IT people. Janna gave us the IT support we required to integrate the system and provided the training our staff needed to operate the system," says Blickensdorf.

ITC replaced the cylinders in their mechanical locks with electronic cylinders. They have installed electronic locks on their RTU and NetShelter cabinets and control-house doors. Electronic padlocks are protecting their TMedic boxes and perimeter fence gates. "The physical cyber assets we are protecting with the electronic locks are critical under the CIP Reliability Standards," says Blickensdorf.

CyberLock Installed in a Net Shelter Box (Photo provided by Robert Blickensdorf at ITC)

ITC has issued electronic keys to their contractors and employees in the field that need access to substations and other sensitive areas. ITC primarily utilizes a contract work force for their field work. These alliance partner contractors typically work full-time on ITC projects and are tasked with maintaining the electric power grid. They require access to the substations in order complete their tasks. ITC programs each authorized person's electronic key with the access privileges they need to do their particular job.

The use of the electronic key has eliminated issues that ITC experienced in the past with their mechanical keys. Keys were being copied and shared, former employees had keys, and keys were missing and unaccounted for. "With the new restrictive electronic key in the field, we have accountability and an electronic record of where the key has been used, how it has been used, and by whom," says Blickensdorf. Each electronic key is set with an automatic expiration to reduce the risks associated with lost keys. If a key is missing, ITC can quickly deactivate the key or let the key automatically expire.

"Everyone in the industry is working towards CIP compliance," states Blickensdorf. He adds, "The electronic lock system assists us with compliance to CIP standards by tracking individuals that go into locations that contain critical cyber assets." Through the placement of an electronic lock, they can at any point download information from that lock and determine who recently accessed that particular location. Each authorized user's key is programmed to access selected locks at specific locations and only during certain times of the day. The electronic locks and keys audit openings and unauthorized attempts to enter areas that protect electronic data and the equipment it's housed in.

"The electronic lock system provides a two-pronged approach to controlling physical access to our electronic assets. First, we can control who we issue a key to and how the key is to be used by that person. Second, we can track that person's activity at the different sites," summarizes Blickensdorf.

ITC's vision to have the best security measures in place to protect the reliability of their grid continues to grow. By partnering with a capable access control system integrator and taking advantage of today's advances in security technology, they have implemented integrated security systems that will continue to provide the physical security and accountability they require. As government standards evolve and new security threats emerge, ITC is in a strong position to respond quickly and decisively.❑

About the Author:
Andy Hilverda is Vice President of Videx, Inc., a company that designs and manufactures security products and CyberLock electronic lock systems.

[1] www.NERC.com