CYBER SECURITY AND DATA THEFT:
THE EVER-EVOLVING THREAT TO WATER/WASTEWATER UTILITIES

Steve Smuda | Wastewater Trainer/Technician

By now I would hope that many people reading this article have at least heard the term Cyber Security and associate it with their water utility in some way. There have been numerous reports and news stories written on big box stores like Target and Home Depot and the theft of consumer's private data. There has been a seemingly endless list of online data breaches involving large servers like Google, Yahoo and Verizon. Wikipedia maintains a list of data breaches that include 30,000 or more records. Why should this concern the operator of a small water plant in Rural NY? The answer may not lie in the information which your system is producing or storing but may be the way in which the system computers communicates with you.

In November 2016 and continuing thru January of 2017, hackers seized control of a water authority's routers and used them for their own transfer of data and internet service. The hackers had no intention of disrupting water flow, gaining access to chemical feed pumps, nor did they even attempt to gain access to any customer information stored on the authority's computers. The hackers only interest was in gaining access to valuable internet service with which to transfer their own data. What problem does this data transfer cause for the water authority? Let's look at it in the terms of monthly data charges the water authority saw before the data breach. The water authority was using seven routers for monitoring remote pump stations. These seven routers were costing the water authority $300 per month for data transfer prior to November 2016. In December of 2016, the data bill soared to $45,000 and then in January 2017, it again jumped to $53,000. The breach came thru just four of the seven routers the authority was using. It is thought that the hackers were able to access the routers thru a factory-installed password. The company which produced the routers had released an update for the router software called a "patch" in May 2016, which would have closed the easily accessible back door to access the router.

The ease with which the hackers were able to gain control of the routers should cause concern for operators of water, wastewater, and other utilities. Many operators don't understand how their remote access systems work nor have they ever seen a utility bill or even know that their utility pays for internet service based on the amount of data used. This could be an inexpensive fix for the utility. It starts with educating employees. By having employees review the monthly bills including monitoring the data usage, they can help build a baseline for the amount of data each system uses each month. Upon installation or shortly thereafter, someone from the utility should begin to monitor and review the information systems and how they are performing. This review should include getting to know the hardware used in the system such as routers, laptops, remote SCADA devices etc. Having employees get familiar with the operation of the utility data systems will help the utility provide a line of defense against cyber attacks and data breaches. The justification for the increase in labor spent on vigilance and maintenance to the information systems may be difficult to put into words for board members. Success in creating and maintaining secure data systems will mean that nothing out of the ordinary happens. Vigilance and maintenance as with all aspects of a water system will help to protect a utility's data system against failure.