Among the big events of the past month is an issue that affects water and sewer utilities: the hack of the Oldsmar water plant in early February. The hacker accessed the plant’s controls and adjusted a chemical feed system, which created a potential health risk to the community. The good news is that an operator noticed that something had changed and called authorities. The FBI confirmed the hack. So how did this happen and can it happen again?

Technology: A Help and a Hinderance

Technology is great, but it has both benefits and challenges. It allows us to gain data on our systems and to use that information to improve operations. As time has marched on, operators and others have sought more and more data, and more people have wanted to access and use that data. Administrators, public safety personnel, regulatory agencies, and others all have asked for access as they saw the opportunities to use the internet of things (IoT) to answer the unknowable, although most barely scratch the surface of the actual data.

As more data can be gathered, the systems have become more complex, which means more access is needed. There is more need for access for information technology (IT) personnel and others to maintain the system through backdoor access points. That means wired and telephonic access, which opens the doors for unauthorized people to access the system.

System Vulnerabilities

Most water and sewer personnel do not readily think that their job includes managing risks (risk managers aside, as they are focused on liability risks from incidents caused by or incurred by the utility, such as workplace accidents—not water supply risks). Instead, we spend a lot of effort on the engineering, operation, and business aspects, but less on planning or risk/vulnerability assessments. The U.S. Environmental Protection Agency (EPA) has required vulnerability assessments in the past, but having done some of those exercises, most are put on a shelf and forgotten. I have had clients ask me if I still had copies because they did not.

We need to keep in mind that there is vulnerability across the entire utility. Vulnerability starts with water supplies, and groundwater is particularly tricky since it’s normally not on the plant site. Aside from the significant decreases reported by the U.S. Geological Survey (USGS) with regard to water levels in many aquifers across the U.S., especially confined aquifers in the western part of the country, their remoteness creates opportunities to hack the system. Technology to monitor water quality to address the ongoing potential for aquifer contamination in your wellfield is another opening for a hacker.

The water plant is an obvious target, as happened in Oldsmar, but wastewater and power plants have similar concerns. For years the federal government has been concerned about foreign and domestic hackers interfering with the power grid. Hackers have been able to penetrate the grid on a number of occasions. That means your high-service pumps, meters, and tanks are all entry points to the system. Wastewater telemetry is vulnerable as well. It’s why we need backup power, but that could be hacked as well if connected to the internet.

Cities have been held hostage by ransomware from hackers. Entry via the billing system is one access point. Ransomware is big business, and lucrative, otherwise no one would bother. The more we spend, the more they spend, just like the drug war. Our 24/7 data is great, until it’s not.
All Grids Are at Risk

The energy grid gets a lot of attention; the water sector is less considered but just as critical, and both are more fragile than we think. As a result, if either crashes, it creates significant potential for economic and social challenges. We need look only at the aftermath of hurricanes or the recent snowfall and freeze in Texas to understand the challenges with a grid shutdown.

The grid in Texas could not produce enough power for heating homes. Natural gas heads froze, and so plants shut down. The system was advised to winterize 10 years ago, but it didn’t. So, like 2003, the grid crashed, sending millions into a power outage. Water utilities, which for some reason did not have backup power, crashed as well.

Hackers can do the same. One operator’s solution is to pull the wires out of the wall, and remove the Bluetooth access at the plant site—therefore, no electronic access. He has argued that administrators do not need access as the plant is staffed around the clock. The site has cameras and alarms both inside and outside; these are patched into police computers, but are not connected to the water plant’s operation computers.

He has a point. Access to real-time data is great, but carries a risk. He is not willing to take the risk or put his customers in danger. What is the value of 24/7 real-time access to people not at the plant site? It’s not like they are making operating decisions from home, nor are they needing data for analysis and reports at midnight or over the weekend.

We can get that data directly from the plant when we need it during the day, but do we really need all that access? We need to think about this.