Overcoming Adversity

Lancaster Area Sewer Authority withstands cyberattack during pandemic response.

Just about the time the Lancaster Area Sewer Authority (LASA) was closing its public office and moving administrative staff to remote work in response to COVID-19, the district was hit by a ransomware attack.

Malware infiltrated certain aspects of the authority's network, locking up systems at perhaps the worst possible time.

"It was hurt on top of hurt," says Mike Kyle, executive director of LASA, which provides sewage collection and treatment to more than 38,000 households and businesses in Pennsylvania.

As a result of the attack, LASA reverted to manual operation, but the staff was able to navigate the event without service disruption or permit violations, Kyle says. The attack also affected aspects of LASA's administrative systems, including its ability to collect online payment for services rendered to customers.

"You have no idea how much you rely on technology until you have none of it," says Kyle. "Even our voice over IP phones were offline, so our customers couldn't call."

Fortunately, LASA has cyber insurance and was able to work with a team offered through the provider insurance to recover from the attack. It took about a month to return to normal operations. LASA has since layered in additional cybersecurity protections. Coincidentally, LASA also had begun working with a third party to revise its cybersecurity plan when the attack hit.

The cyberattack turned Kyle into an evangelist for cybersecurity awareness for wastewater agencies and other special districts.

"I'm an advocate now and a preacher for comprehensive cybersecurity plans, because it's not a question of if you'll be attacked, but when," he says.

Growing Threats

The type of cyberattack that hit LASA is becoming more common among public utility districts, says Michael Harrod, a principal architect with AT&T Public Sector. That's because traditionally standalone industrial control systems, known as supervisory control and data acquisition (SCADA) systems, are being connected to enterprise wide area and local area networks.

"Integrating SCADA systems into IP-based environments brings a lot of intelligence and other new functionality," Harrod says. "But they do become more vulnerable to attack."

Today, IP-enabled SCADA systems and the networks they reside on must be covered by the same cybersecurity protections that safeguard general information technology systems and communications networks.

"You really can't treat them separately," Harrod says. "They need to be integrated into your overall security posture and plan."

Comprehensive security plans have become more important as well, as the volume and sophistication of cyber threats

increase. Harrod says organizations must first understand all elements of their technology environment — including internal resources, cloud-based solutions and third-party partners. They should also work with a security specialist to perform penetration testing to identify vulnerabilities that must be addressed. Developing an effective plan helps districts prioritize security activities, ensuring they get the most value from their investments.

"It can be like drinking from a fire hose when we talk about security," Harrod says. "It's all about looking at these steps in a very logical way."

With proper security, however, public utility districts can benefit greatly from adding network connectivity, sensors and intelligent software to traditional operating infrastructure.

"The whole arena of IoT [Internet of Things] and smart devices is a game-changer for these organizations," Harrod says. "You can put smart devices into areas that are difficult to access and automate processes that require a lot of human intervention. You can monitor tank levels or water flows; you can use cameras or other devices to understand true metrics."

He adds that new connectivity technologies like 5G will safely support expanded use of IoT devices in water and sewer systems and other public utility infrastructure. 5G offers built-in security, as well as sufficient bandwidth to support massive numbers of sensors, he says, making it an ideal foundation for smart device networks.

Efficiency and Innovation

LASA already uses various technologies to improve efficiency and reliability of the sewer system. For example, the organization uses acoustic sensing devices to assess the condition of underground sewer pipes and hunt down clogs. The tool analyzes sound waves as they travel through the pipes to spot potential problems.

"We've dramatically reduced the amount of pipeline that we flush or clean, because we can target our maintenance," Kyle says. "It's much quicker and cheaper to inspect a thousand feet of pipe using this method than it is to routinely flush a thousand feet of pipe. We've really been able to optimize our cleaning crew to focus on the areas that need cleaning."

LASA also uses video monitoring and remote data collection technologies, such as sensors on manhole covers that alert operators to high water levels. Use of these devices is poised to increase as LASA grows its service footprint. The organization currently has 38 pump stations and is actively acquiring smaller sewer system operators in the area.

"We have a proliferation of very small systems in our area that just aren't sustainable, so there's a trend toward consolidation," Kyle says. "We're pretty spread out, and we'll get even more spread out as we acquire systems. It gets very costly to have people in the field monitoring those assets."

With enhanced security protections and plans in place, LASA is positioned for success. Kyle expects more innovation as the authority seeks to manage expanding assets efficiently and effectively.

"That's really the trend," he says, "and it includes bringing in technology and using it the right way."

Market Overview:
Sewer Districts

SEWER DISTRICTS FACE GROWING CYBERSECURITY CHALLENGES as they automate and connect formerly standalone industrial systems and infrastructure. As these assets are brought into IP-based network environments, they increasingly are vulnerable to attack. Malware now can enter enterprise IT networks through weaknesses in industrial control systems, causing widespread disruption.

Sewer districts — and other operators of public utility infrastructure — must make sure emerging sensor networks, automated plant controls and other smart infrastructure devices are protected by the same security measures used to safeguard other technology assets. They'll need to work with security experts to perform appropriate vulnerability testing and develop comprehensive plans for remediating security gaps and monitoring evolving threats.

On the other hand, smart automation and IoT devices offer tremendous benefits to sewer districts when used with the proper security measures. Connecting and adding intelligence to plant equipment, pump stations, pipelines, valves and other assets enables these districts to operate more efficiently and collect real-time data to improve decision-making. These efficiencies are particularly important now, as the COVID pandemic reduces revenue for sewer system operators and a trend toward consolidation increases the amount of infrastructure managed by individual organizations.

To learn more about how special districts are innovating across the nation, visit: govtech.com/districts