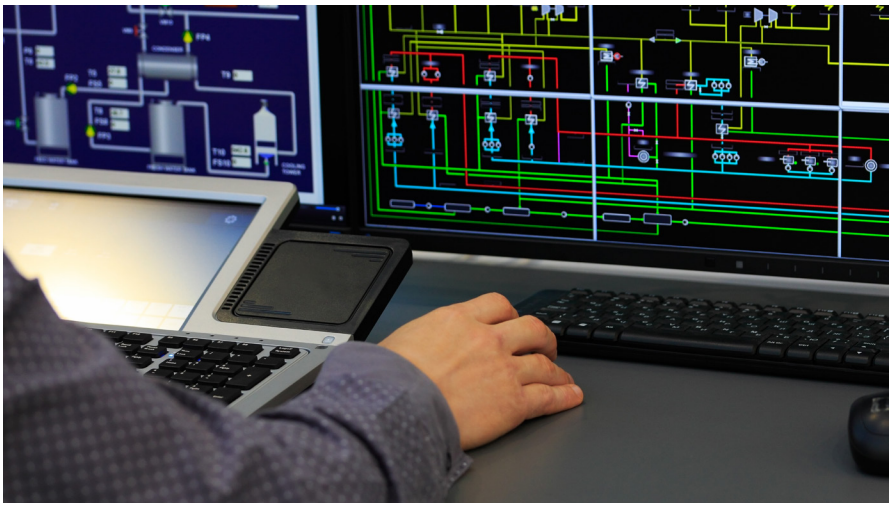
FLORIDA CYBERATTACK RAISES PUBLIC AWARENESS OF THREATS TO WATER PLANTS

An ES&E Special Report



As utilities increasingly take advantage of the automation available through modern SCADA technology, they will also need to upgrade their cybersecurity measures to protect their more technologically-advanced systems. Credit: gen_A / AdobeStock

A cyberattack that nearly poisoned a Florida water plant in February has utility security professionals reassessing their readiness for digital threats. Threats from virtual intruders that go beyond typical IT targets such as compromised customer accounts, and enter the more dangerous realm of sabotaging a plant's core operations.

Computerized control systems, known as OT (operational technology), are the critical systems for utilities that look after tasks such as monitoring/controlling process equipment, logging key regulatory data, and providing interface screens for operators to make system adjustments. Most OT systems, unlike IT infrastructure, can never be turned off because they control process equipment and safeguard critical control points.

While considered to be a near miss by many industry professionals, the recent Florida plant attack served as a potent reminder of what can happen when an OT system is compromised.

On February 5, 2021 in Oldmsar, Florida, a hacker compromised a remote

access interface, taking advantage of the plant's OT system to spike sodium hydroxide levels to over 100 times the normal dosing rate. Sodium hydroxide, commonly known as caustic soda (NaOH), in small quantities is an effective pH correction chemical, but in large quantities can be fatal.

Fortunately, it was a near miss. The Florida attack was unsophisticated in nature. A plant operator happened to be in the right place at the right time to notice the process change and was able to shut down the process before the water reached any customers.

CYBERSECURITY RISKS AND PUBLIC PERCEPTION

For the public on the outside looking into our utilities, the increasing volume of cyberthreats is worrying. Furthermore, it can be difficult to differentiate between protecting against hacks of a facility's information focused IT systems versus its operationally focused OT systems.

Many people have read about hacks in the news, such as the recent breach that compromised nearly a million Canada Revenue Agency accounts. These are considered cyberattacks on information technology, or IT, which can affect elements such as websites, data records and email systems.

"The stakes involving cyberattacks on OT, however, are generally much higher than those surrounding IT," says Graham Nasby, a water SCADA and security specialist with the Environmental Services Department of the City of Guelph, Ontario.

This is because OT systems, such as SCADA (the plant's supervisory control and data acquisition) system, need to function continuously in order to keep process systems working properly. Regardless of the utility type, whether it be water, wastewater, electricity or gas, each will have SCADA systems as part of the OT they depend on.

"The way you deal with cybersecurity for an OT system is completely different than for IT," says Nasby. "An OT system—you can't turn it off. OT systems are pumping your water, treating your sewage, producing electricity, delivering gas and controlling infrastructure-critical processes. If a hacker gets into an OT system, critical services the public depends on can be compromised."

Some parts of OT systems are more vulnerable than others. Many OT experts considered the Florida attack to be relatively unsophisticated because only the user interface was targeted. A more insidious type of attack could have targeted the underlying control system hardware of the SCADA system, which could have done considerably more damage and likely not have been noticed by an operator until it was too late.

continued overleaf…

However, brushing up on the current best cybersecurity practices can help utilities prepare for what could be more covert attacks in the future.

"The threats and the knowledge of how to best protect systems against them are always evolving," says Nasby, who sits on several international technical committees that write cybersecurity best practices for control systems.

Of the ongoing debates within the cybersecurity sector, one that continues to challenge utility systems, is how to best secure remote access to systems. Notably, in relation to the Florida hacking incident, a *Wall Street Journal* investigation revealed that just three months earlier, the utility had passed and completed a U.S.-based federally required security assessment. However, it had yet to implement the findings and recommendations from that assessment. Since the attack, the Florida plant's owners have removed the remote access connection that was the entry point for the intruder.

"Deciding whether to implement remote access to OT systems is a challenging issue to manage," says Nasby.

While it can be operationally very convenient for the utility (as it avoids operators having to travel to locations with SCADA terminals to make process adjustments), it also exposes the utility to risks, such as those recently demonstrated in the Oldsmar attack. If the decision is made to implement remote access, it is something that has be designed, implemented and monitored very carefully.

"Smaller utilities also face additional challenges. Due to their smaller revenue base, they typically have less resources available to secure remote access. Yet, with their smaller operational teams and often spread-out geographic areas, there can be real operational benefits to having remote access. However, before remote access to OT systems can be considered, how to mitigate security risks has to be very carefully reviewed," says Nasby.

"You need to look at an entire system and ask, 'how am I only going to allow access to authorized users?' If they're able to get in, do we give users keys to the entire castle, or do we restrict them to a certain area? And how do we decide how many layers of security will be needed?" asks Nasby.

What this means is that if remote access is being considered, it is something that must be designed into the system. Current OT cybersecurity best practices require that multiple layers of security be used for protecting these critical systems. These often include multiple layers of authentication, encryption, multi-factor login accounts, and segmenting the control system network into zones.

Depending on the type of process, this may also include using additional backup controllers (not accessible via the control system network) to provide backup control for critical processes.

Additionally, automated monitoring, change control and backup systems are also needed to continually monitor the system. In a well-designed system, an authorized user would need to pass through numerous gates to gain access, and any access granted would be continually monitored, logged and reviewed.

"Within each layer, you progressively gain more access. There may also be parts of the system that you don't allow remote access to at all because the risk is too high," says Nasby.

For any utility, protecting OT systems from cyberattacks is a challenging undertaking. Furthermore, effectively designing and implementing cybersecurity countermeasures is a specialty skillset. It is an area where utilities should not hesitate to bring in specialty service providers to help them secure their systems.

Cybersecurity is also something that must be designed into each system, as each system is unique, based on the particular processes being controlled and the individual utility's needs. It is not just a case of installing "cybersecurity software" or adding in a "remote access package."

"In terms of cybersecurity software and monitoring services, it is, unfortunately, still very much the Wild West when it comes to the marketplace," says Nasby.

Many available products and services may appear to be suitable, but fall short when subjected to a close technical evaluation and/or compared against actual operational scenarios.

There is also an important distinction to be made between proactive products and services (to help prevent an attack) versus reactive ones (that would

only notify you of a suspected attack but do nothing to prevent it). Many of the products that claim to be a comprehensive solution fall into the latter category. There are also a lot of false promises out there, so it is important to do your homework when looking at these products and services.

"With that said, there are a number of proven products that can be used to help secure OT systems, but in every case, they have to be deployed with a larger and carefully planned multi-faceted approach. There is no magic bullet," Nasby cautions.

Every utility situation is different when it comes to cybersecurity, and a lot of it depends on the individual utilities' needs, size, funding and operational resources. Some utilities have decided to not offer remote access to their OT systems, as they feel it is not worth the risk. For others, they have invested in building their own private radio, cellular or fibre networks so they don't have to expose their systems to remote access via the Internet.

Other utilities have chosen to offer remote access via the Internet but they have invested heavily in sophisticated multi-layered protection schemes to ensure that only those authorized to do so can gain access.

For utilities out there that have not yet reviewed their cybersecurity stance, there are fortunately several resources available. There are also a number of specialty OT-focused cybersecurity service providers that can provide advice and services to help guide utilities as they continually adapt to the ever-changing cybersecurity landscape.

Interestingly, as SCADA systems are added and upgraded—with evermore features and capabilities—sometimes the new functionalities offered by modern SCADA systems can create new cybersecurity risks that must be managed. As more and more smaller utilities take advantage of the automation available through SCADA technology, they will correspondingly also need to upgrade their cybersecurity measures to protect their more technologically-advanced systems.

For example, if a utility were to move from a monitor-only SCADA system to one that does active control, additional cybersecurity protections would be needed. Likewise, if a utility moves from a closed-access SCADA system to one that offers remote access, the corresponding cybersecurity countermeasures to safeguard the remote access vector must also be upgraded.

All of these considerations, and the continually evolving cybersecurity landscape, underscores the need for utilities to ensure they make use of a well-versed OT-focused cybersecurity expert, whether it be via a specialty service provider or in-house SCADA staff, to help guide them when it comes to managing cybersecurity risks. The risks and industry best practices are always changing, so it is important that the most up-to-date knowledge, skills and experience are always being used.

Ultimately, there is a direct tie between a utility's funding model and how well it can manage cybersecurity risks. Managing cybersecurity risks effectively is something that requires ongoing resources, including staff time, funding and technology. Just as the cybersecurity landscape continues to evolve, utilities must continually invest in and evolve their cybersecurity countermeasures to keep their OT system online and protected.

Cybersecurity can be challenging as it can be hard to "see" versus physical infrastructure, but it is just as important. Education and awareness are also part of the puzzle. Fortunately, says Nasby, "there is an ever-growing body of cybersecurity knowledge that can be leveraged by both technical folks and utility managers alike towards the common goal of keeping our critical utilities safe and secure." ■

ES&E would like to thank Graham Nasby for his assistance and expertise in writing this article.

For a list of references and links to the mentioned cybersecurity resources and best practices, visit: www.esemag.com/april-2021-cybersecurity, or email editor@esemag.com.