Bond Case Briefs

Municipal Finance Law Since 1971

Hackers May Be Coming for Your City's Water Supply.

More digitized and connected than ever, the nation's infrastructure is vulnerable to cyberattack.

I first saw the inside of a water-treatment plant in 2015. I was conducting a site visit at a municipal facility in New Jersey, where I was the state's director of cybersecurity. It wasn't an inspection; the plant manager had asked me to visit.

Changes at the facility over the years had made him uneasy. Analog machinery had given way to digital systems, and critical water-treatment processes were now automated. The plant required little human intervention in day-to-day operations. Thanks to remote-access technologies, more maintenance and monitoring activities were being performed off-site by a third party. All this was great for efficiency, especially for his resource-limited operation, but what about the risk? Optimizing for cost and speed meant connecting more digital and networked technologies to his plant floor. Security was no longer simply a matter of gates, guards and guns. It had become a matter of bits and bytes.

In early February that plant manager's unease became another's reality when someone reportedly tried to poison the water supply in the Gulf Coast city of Oldsmar, Fla. According to the Pinellas County Sheriff, a hacker gained remote access to Oldsmar's water-treatment-plant network and briefly increased the amount of sodium hydroxide in the water by 100 times—enough to cause death or serious injury to anyone who drank or touched it. Thankfully a technician noticed the anomaly and booted the hacker off the network before any damage was done.

What happened in Oldsmar fell just short of the nightmare scenario. The average person is unaware how dependent the country's critical infrastructure has become on digital technology. At power plants, waterworks and all manner of public utilities, special-purpose computers known as human-machine interfaces connect to ruggedized-process controllers that regulate actuators to spin turbines, rotate robotic arms or, in this case, open valves to release sodium hydroxide.

In a perfect world these communications and the operations they command would be walled off from internet-connected systems. But practical demands to monitor operations in real time, glean data analytics from the plant floor and perform remote maintenance have in many cases exposed vulnerable infrastructure to the other side of the firewall. The result is more web-based hacks of operational technology systems. The bad guys get access to critical infrastructure facilities when corporate devices are inadvertently connected to the internet or a network administrator's credentials are stolen in a spear-phishing scam.

Oldsmar wasn't the first cyberattack against water infrastructure. In April 2020 Israel's National Cyber Directorate urged all water-treatment companies to change their passwords on critical systems. In 2016, according to a report by Verizon's security unit, hackers with ties to Syria gained access to a water utility in an unknown country and managed to "handicap water treatment and production capabilities."

Despite the alarmist headlines, Oldsmar is mostly a good-news case study. The treatment center swiftly identified what was happening and took immediate action to keep the poison out of the public water supply. Even if the plant hadn't responded as quickly as it did, there were other controls in place that would have detected a problem and maintained the system's integrity.

But redundant controls and a bit of good luck shouldn't diminish the severity of this cyber threat to public health. The plant operator was tipped off by a mouse arrow moving across a screen and making changes to critical water-treatment processes. But what if the operator didn't have the benefit of a visual aide to observe the hacker in real time? What if the human-machine interface was manipulated by malware to report "all clear" as the hackers increased concentration of sodium hydroxide to lethal levels? Would the breach have been detected before someone drank or bathed with the corrosive adulterated water?

The answer and the problem are inextricably linked. Detecting toxic water en route to consumers requires sensors in the distribution network. Those sensors must be connected so they can communicate and transmit data for either humans or machines to take preventive actions. Anything that is connected can be manipulated. Should we rip the sensors out lest they be hacked? Of course not. Instead we must reduce vulnerability by extending security to all parts of the network, even those that seem beyond the reach of malicious actors.

"I just don't trust those computers," the New Jersey plant manager told me in 2015. We should all be untrusting when it comes to technology, but not at the expense of its embrace. The zero-trust mind-set made all the difference for the city of Oldsmar.

The Wall Street Journal Opinion

By Dave Weinstein

Feb. 26, 2021 5:53 pm ET

Mr. Weinstein is an associate partner at McKinsey & Co. and former chief technology officer of New Jersey.