Cybersecurity Importance On The Rise In Water Utility Operations

Image credit: "Hacker Hacking Password With Magnifying Glass and Binary," Mike Corbett © 2018, used under an Attribution 2.0 Generic license: https://creativecommons.org/licenses/by/2.0/

As water utilities migrate toward remote system monitoring and control in real time, the risks associated with cybersecurity tick upward as well. While the rewards of digitalization offer real promise, the associated complexity and concerns pose corresponding risks. That is why it is important to have an overall risk management process for the organizational level, for the business process level, and for the information systems and data levels as well.

Defining The Problem

Cybersecurity is not just a financial or communications industry concern. With the growth of industrial control systems (ICSs), the number of risks in the industrial and utility sectors has grown exponentially over the past five to 10 years. From RF-based plant and distribution control systems to smart meters, the desire to improve ICS operating efficiencies through automation and digitalization has superimposed specific new considerations on top of the basic IT cybersecurity challenges.

In the world of water utilities, the systems, data within those systems, and access to those systems are all cyber assets and should be evaluated as such. According to a recent *Wall Street Journal* article, the Department of Homeland Security reported earlier this year that foreign operatives gained access to U.S. utilities by penetrating the networks of trusted vendors to those utilities.

From data breaches to service interruptions in consumer and commercial environments, ICS users in the utility marketplaces are becoming more aware of the risks of cybersecurity incidents than ever before. Gone are the days when organizational leadership could say, "We've air-gapped our systems, so we have eliminated external risks and threats."

Where To Start?

Any water utility operator tasked with the chore of doing more with a smaller budget or fewer experienced personnel is going to be interested in ways to automate the process securely. The informative white paper *Securing Industrial Systems In A Digital World* is an excellent starting point. It addresses the state of the industry, outlines the impact of real cyber attacks, and identifies regulatory requirements. It also identifies steps for taking cyber asset inventories and best practices for measuring cyber risk and identifies specific strategies for effective risk management and implementing baseline security measures within ICS organizations.

It is important for cybersecurity to be aligned with an organization's larger digital and enterprise risk strategy. This executive report on resilience for process control systems further addresses the differences between cybersecurity

planning for process control IT vs. corporate IT and the need for the two disciplines to work together.

Six Principles Of Cybersecurity Protection

Regardless of any specific industry standards involved — IEC 62443 2-4, NIST 800-53, ISA-99, NERC-CIP, etc. — the following principles of cybersecurity protection provide a road map for utilities interested in building more secure and resilient systems:

- Identify. Pinpoint not only potential threats, but also corresponding executive support for programs and funding to execute appropriate cybersecurity responses to those threats.

- Protect. Minimize exposure to vulnerabilities with products, services, and protections designed to intercept and mitigate the impacts of potential threats if they do arise.

- Detect. Don't wait to be reactive to cybersecurity intrusions. Rather, maintain an ongoing active role in assessing and managing potential threats and vulnerabilities.

- Respond. Have defined processes and procedures to respond once a particular type of vulnerability or threat is detected and hold periodic exercises to train incident response personnel on executing those procedures.

- Recover. Ensure that backup and restore processes and practices are well developed and established to restore the system as close as possible and as quickly as possible back to where it was before the cybersecurity incident.

- Comply. Conduct regulatory compliance training and routine audits to establish a basic level of cybersecurity maturity, then maintain and ultimately improve upon it, year after year.

- Whatever a utility's status or rate of progress toward these objectives, however, cybersecurity is not a destination; it's a journey. That is why rigorous up-front evaluation and planning are just as important for establishing methodologies to prepare for future unknown challenges as they are for meeting current challenges.

Planning The Next Steps

Consider these tactical steps for achieving the strategic goals outlined above, as part of a larger methodical approach toward protecting water utility operations:

- Security Assessment And Monitoring. Compare current assets and levels of protection against industry standards and best practices.

- Perimeter Protection. Firewalls working hand-in-hand with a well-designed security policy can separate networks into distinctly controlled and protected zones.

- Security Updates And Hardening. Efficient patch management is essential. The ongoing process extends well beyond antivirus software to include operating systems and embedded software.

- Procedures And Policies. Work hard to develop and communicate processes and procedures to detect and deter threats among interconnected systems on a global basis.

- Malware Protection. Equip substation automation systems with industry-standard intrusion protection and malware protection solutions, antivirus protection, and application whitelisting.

- Backup And Recovery. Secure offsite backup systems to make recovery easier, whether security attacks or other problems compromise access to critical data.

Automating Real-World Cybersecurity Solutions

As both ICS capabilities and their corresponding cyber threats become more complex, the value of having a cyber asset inventory becomes more obvious. Because performing a cyber asset inventory manually is so time-consuming, and because any such inventory is basically outdated as soon as it is completed, it is extremely valuable to automate that process.

Using a vendor-agnostic automated cyber asset management tool that runs in real time to develop a comprehensive asset inventory can aid water utilities in responding to potential threats, regardless of the technical experience of their workforce. Equally important, automating that inventory instead of performing it manually can reduce staff effort by up to 120 hours per month.

Beyond the cyber asset inventory, automated cybersecurity monitoring services that compare ICS system data against industry best practices and standards can also pinpoint areas of concern for utilities that are new to cybersecurity implementation. ■