# How to Incorporate Cybersecurity Into the Utility Master Plan

A protective, cost-effective approach to risk mitigation

By Umair T. Masud

Massive cybersecurity breaches make headlines on a regular basis. These constant reminders of potential system vulnerabilities can be particularly troublesome to those charged with safeguarding the public's water supply.

With limited staffs and budgets, utilities often must postpone comprehensive upgrades, evolve their industrial control systems (ICS) and IT infrastructure slowly, and rely on external expertise.

Still, water utilities can take steps now to better mitigate risk through a proactive approach that extends beyond regulatory compliance—and makes ICS security part of the utility master plan.

## Change the Mind-Set

Utilities tend to view any initiative related to ICS and IT as a "project." And virtually all have taken a project approach to implement passive cyber defenses, such as firewalls and email filters. But when it comes to cybersecurity, a "set-it-and-forget-it" project mentality can be dangerously limiting.

In today's world, cyber threats continually are evolving and escalating—and can impact every aspect of a utility. To be truly effective, cybersecurity must be based on an agile and active defense strategy that extends through every project in parallel with all business operations.

It is time to change the mind-set: Cybersecurity is an ongoing "process," not a project.

## Lay the Foundation

For some water utilities—which have a high volume of critical assets, plus complicated governance—the scope of an ICS security program can be daunting.

However, regardless of infrastructure size or complexity, all utilities face similar challenges. And all can deploy a common, proven methodology to mitigate risk.

That methodology must:

- Begin with an assessment of business needs and the specific operational requirements of the process control system;
- Identify critical assets and data that are essential to operation;
- Support asynchronous technology and business change;
- Recognize that no single product or technology will fully secure industrial networks and that the most secure posture will always require people (e.g., analysts); and
- Utilize a "defense-in-depth" strategy based on multiple countermeasures that disseminate risk over an aggregate of security mitigation techniques.

## Get Executive Buy-In

Identifying the right team to support and execute this methodology is critical. To be effective, this team must be endorsed at the executive level—and include expertise encompassing both the ICS and business-level networks.

Ideally, this team will be charged with formalizing and executing the policies and procedures that will guide the utility on cybersecurity issues for years to come.

## Set Strategic Priorities

Assessments are the starting point for any cybersecurity program. Through an assessment, a utility can determine what is "normal" from the standpoint of data entering and leaving the system. This is a crucial first step to identifying abnormalities and potential security events.

In addition, an assessment evaluates a utility's security practice architecture and its ability to protect ICS assets.

Effective security assessments also extend beyond the technology deployed and take into account existing policies, procedures and typical behavior.

At minimum, an assessment should include:

- An inventory of authorized and unauthorized devices and software;
- Detailed observation and documentation of system performance;
- Identification of tolerance thresholds and risk and vulnerability indicators; and
- Prioritization of each vulnerability, based on impact and exploitation potential.

The outcome of any assessment is a prioritized list of mitigation activities.

## Align Investment With the Master Plan

With prioritized mitigation steps in hand, a utility is ready to implement a cybersecurity program. However, justifying funding often is fraught with challenges.

First, the benefits of a cybersecurity program are usually invisible and can only be tracked through metrics. It is easier to justify additional costs or to divert funds for improvements that directly impact water delivery or quality.

In addition, cybersecurity is not a one-time expenditure. It is a commitment that commands vigilance and an ongoing investment in people, process and technology.

Due to these factors, aligning critical security controls investment closely with the utility master plan is the most effective, publicly palatable and fiscally responsible approach.

## Ways to Align

While not an exhaustive list, here are some specific ways a utility can implement a strategic, lifecycle approach to cybersecurity investments:

- **Biggest impact first.** Follow the initial assessment prioritization and allot funds first to those investments that are most critical.
- **Assess all cyber investments for risk.** Most utilities include risk assessments as part of the selection process for physical infrastructure investments. Extend this mind-set to investments that affect the IT infrastructure and ICS.
- **Invest for a more secure future.** Make "future-ready" ICS and IT investments at every level of the enterprise. Select technology that incorporates cybersecurity features, even if those features cannot be immediately activated.
- **Scrutinize and limit system proliferation.** Narrow the scope of system suppliers and service level agreements. The fewer disparate systems within an environment, the easier it is to secure them.
- **Consider Quality-Based Selection (QBS).** This pre-selection procurement system focuses on the long-term lifecycle costs of a solution—not only up front capital costs. QBS helps set a technology direction for the future that prioritizes an integrated secure environment.
- **Recognize the value of ongoing and annual assessment.** A successful cybersecurity strategy requires an ongoing audit of what exactly is occurring in the system and an annual assessment to restate or realign priorities.

## Positioned for the Future

On the surface, water systems may not appear very different from the day they were commissioned. But chances are, the inner workings of these systems have radically changed. Often, there is a tremendous intermixing of old and new products—and various creative methods to exchange information.

Within this environment, understanding even the current system security baseline can be a challenge. However, the need to address cybersecurity issues has never been greater.

By aligning critical security controls investment with the master plan, utilities are well positioned to identify system vulnerabilities and undertake essential mitigation steps—both now and in the future. **wwd**

**Umair Masud is senior consultant in the network and security services business for Rockwell Automation. Masud can be reached at utmasud@ra.rockwell.com.**