Massachusetts Public Water System Cybersecurity Survey: Analysis and Recommendations

By: Andrew Hildick-Smith*, Gufran Bulbul, and Michael Celona****

*** Principal at OT Sec, LLC and MassDEP Drinking Water Program Technical Assistance Provider**
**** MassDEP Drinking Water Program staff**

No sensitive information is included in this report

Background

Due to the increasing number of cyber-attacks on the water sector, the Massachusetts Department of Environmental Protection's Drinking Water Program (DWP) formulated a cybersecurity strategy to help water systems mitigate potential cyber threats. As a part of this strategy, the MassDEP Drinking Water Program developed a cybersecurity survey to help to better assess and understand public water systems existing cybersecurity issues/risks and identify resources. The survey was sent to all Public Water Systems (PWS) on December 1st, 2021, and two weeks of time was given to complete the survey (Friday, December 17, 2021). The survey was available through the MassDEP webpage.

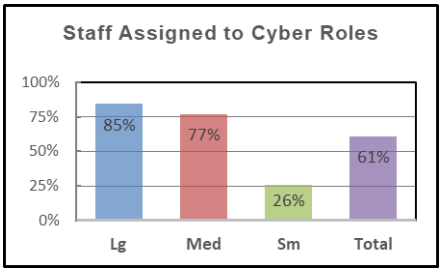
The survey contained 15 questions under three sections: 1- PWS information; 2-Cybersecurity Policies, Procedures, and Manual Operations; and 3- Protective Measures. To ensure the confidentiality of the PWS, the survey was developed in a way that no identifying information was collected such as PWS name, email address, or PWS ID. Also, PWS were informed that responses would not be used for enforcement but that several cybersecurity questions would be added to future sanitary surveys.

The survey was shared with all PWS (approximately 1,600) and a total of 105 responded (7%). While low, these consisted of many systems that use supervisory control and data acquisition (SCADA) or are more vulnerable to cybersecurity issues, specifically 34% of all large-sized systems and 22% of all medium-sized systems in MA. Large systems were defined as those serving > 50,000 people, medium systems as those serving > 3,300 to <= 50,000 people, and small systems serving <= 3,300 people. There categories were chosen to match the American Water Infrastructure Act size categories. Most respondents (80%) were COM systems, followed by TNC (11%) and NTNC (9%). Some small systems reported they couldn't complete the survey since their PWS does not use computer systems.

Response Observations

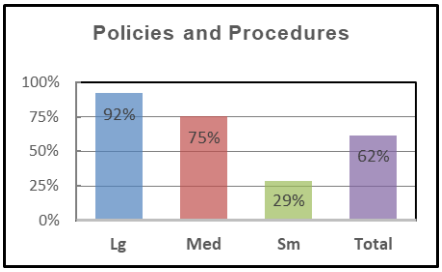
This section of the report looks at the significance of the questions and the results organized by utility size. The graph bars on the subsequent pages represent the percent of affirmative responses by large (**Lg**) systems serving >50,000 people, medium (**Med**) size systems serving > 3,300 to <= 50,000 people, and small (**Sm**) sized systems serving <= 3,300 people. The **Total** bar represents the combined response by all systems.

Staff Assigned to Cyber Roles



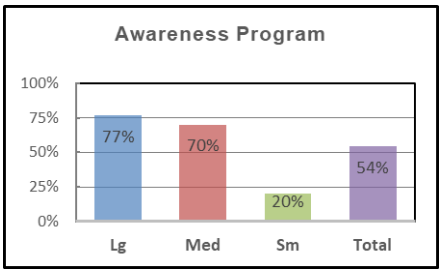
This is probably the most fundamental step for a water utility in developing a cybersecurity program. While it might sound simple, formally assigning a lead and supporting staff is difficult because it potentially requires a job description change and a discussion of perceived liabilities. Having cybersecurity expertise would be valuable but is not a necessity. The lead person needs to be a good manager, and the supporting staff or contractor needs a foundation of basic IT skills to build on. Large and medium utilities had a fairly strong response, with a sharp drop-off by small utilities.

Policies and Procedures



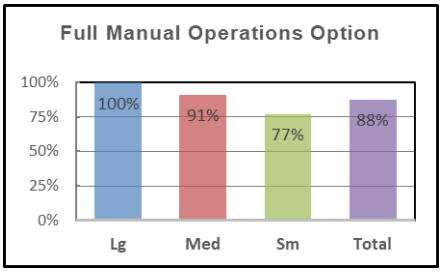
Developing formal cybersecurity policies and procedures is a demanding process. That 92% of the large utilities and a sizable majority of medium sized utilities responded positively to this is impressive. It would be interesting to see what percentage of utilities actually enforce what they have written-which is a whole other level of effort.

Awareness Program



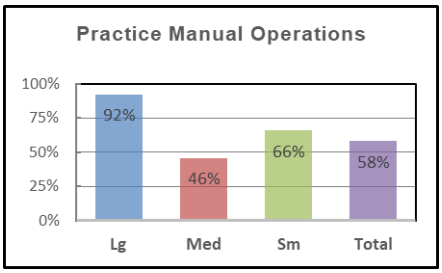
Because all staff play an important role, it is important for every utility to have a cybersecurity awareness program and to develop a strong cybersecurity culture. For cybersecurity awareness programs to be effective they need to be repeated at least quarterly and ideally monthly. Fortunately, awareness programs are relatively inexpensive.

Full Manual Operations Option



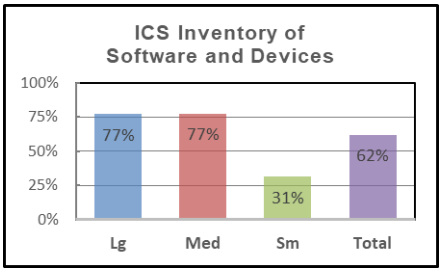
It is great to see the high percentage of all respondents that can run their system manually. This is important from a cybersecurity perspective but also from a normal resiliency point of view. It would be interesting to see if there are many cases where "manual" operations depend on local panel control that includes the use of a networked controller such as a Programmable Logic Controller (PLC). Somewhat surprisingly, smaller systems had fewer manual options, but perhaps cost savings drove a less flexible control solution.

Practice Manual Operations



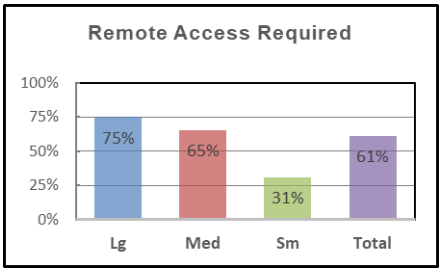
Practicing is important to make sure you can do what you think you can do. It keeps staff familiar with the steps and precautions required to successfully provide safe drinking water without introducing problems. This question was accompanied by a related question that asked how often the utilities practice. There were 6 that responded weekly, 6 quarterly, 14 monthly, 15 annually and 20 "other". It would be interesting to understand how many of these utilities schedule their manual operations versus operating manually because of control system problems, and whether they are running the whole system or just sub-components.

ICS Inventory of Software and Devices



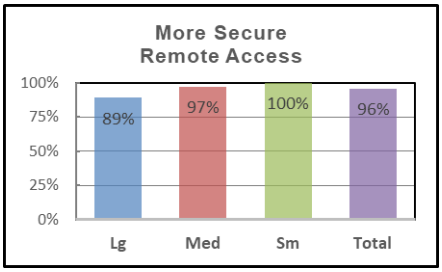
Every utility has a sense of the software and devices that it is dependent on for providing safe drinking water but having an actual list and maintaining it over time takes commitment. After assigning a cybersecurity leader, this is probably the second most important step a utility can take towards having a meaningful cybersecurity program. While the number of instances of a particular item will be higher in a bigger system, small systems are apt to have a similar variety of items.

Remote Access Required



An interesting part of this response was the level of utilities that indicated "N/A". Presumably, that indicates that they do not have SCADA system. There were 22 small systems in this category, 5 medium, and 1 large one, or 26% of respondents. In addition to knowing the number of utilities that require remote access it would be good to know how many others have it as a convenience, but it is not required. Some portion of the utilities that have a SCADA system and responded "no", may use alarm "dial-out" programs for system awareness during off hours.

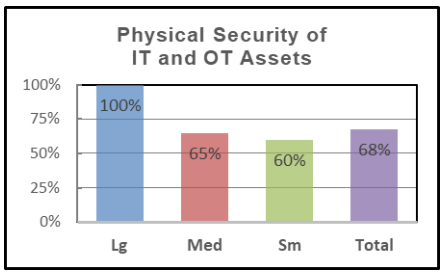
More Secure Remote Access



The survey asked if the utility requires remote access and if so, if it is protected with "one of the following or other comparable methods (multifactor authentication, jump server, virtual private network, etc.)" to get a sense of the level of security. While the responses look very good, perhaps a "Not sure" answer should have been included given the extremely high positive response, especially from the small and medium sized utilities. A follow-up might help understand if PWS use multifactor authentication or other best practices.

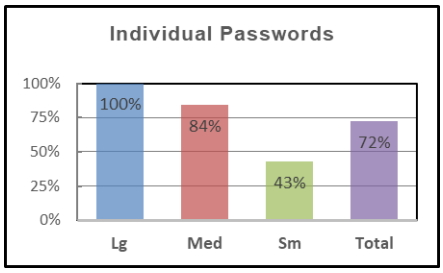
Physical Security of IT and OT Assets

Physical security is a basic measure that water utilities are used to taking to protect their assets and product. It may just be an awareness issue for medium and small systems to extend that same protection to their IT and OT assets. The survey question included in its examples the use of locked server rooms and cabinets and alarms.



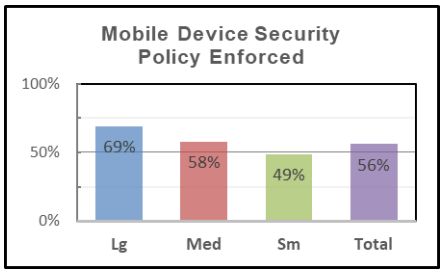
Individual Passwords

Staff accountability and security depend on individual accounts and passwords for both computers and software applications. The use of individual passwords is a basic requirement for cybersecurity. Sometimes the PC interface to a control system at a treatment plant is just left on and open for both convenience and to feel confident that in an emergency access will be both rapid and assured.



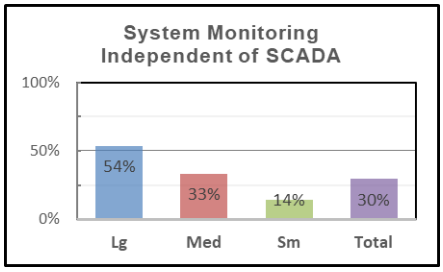
Mobile Device Security Policy Enforced

On the assumption that remote access to a control system may frequently be from an operator's or manager's mobile device, the water system's security cannot be any better than the mobile device's security. Even the most security remote access can be compromised by a hacked phone, tablet or laptop. Non-work use of these same devices greatly increases the risk of a problem.



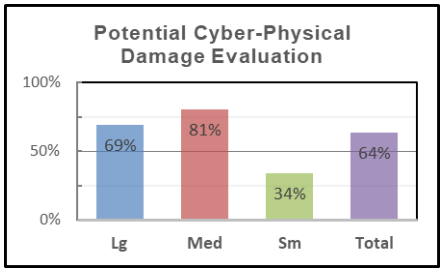
System Monitoring Independent of SCADA

Water system status monitoring with a data logger or other equipment independent of a SCADA system can be a robust way to validate the health or compromise of a SCADA system. It also provides a useful backup to help run a water system manually if the SCADA system is down for whatever reason. Independent monitoring is an advanced approach that is not common.



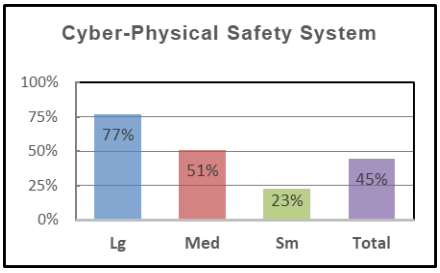
Potential Cyber-Physical Damage Evaluation

It is excellent that this many utilities have thought about which critical systems or equipment might be susceptible to physical damage from a cyber-attack. Hopefully, this question and the next one was understood. It is a little concerning that there is a higher percent of large systems that have implemented a cyber-physical safety system (see below) than have thought about where they are needed.



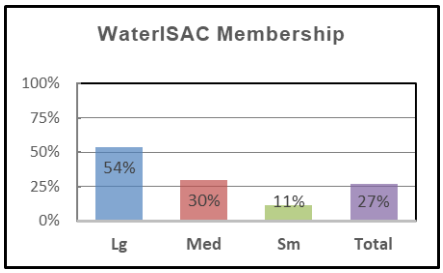
Cyber-Physical Safety System

It is exciting that so many utilities have proactively taken action to prevent a serious cyber-attack from being able to physically damage some part of their system. Following up on what steps were taken and then sharing that information anonymously would be valuable for the water sector regionally and nationally.



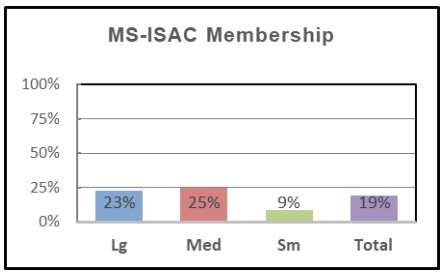
WaterISAC

The WaterISAC provides a very valuable service of twice-weekly reports curated for the water sector that include cybersecurity threats and advisories, all-hazards issues, and training opportunities. High level alerts are promptly distributed. Monthly webinars help with education and encourage best practices. There is an annual membership fee that starts at $100 for small utilities (<=3,300 people) and increase from there. Every water and wastewater system should be a member.



MS-ISAC Membership

MS-ISAC membership is free and provides a number of useful benefits, including reduced cost for advanced cybersecurity training and the possibility of incident response assistance in the event of an attack. Every municipal water and wastewater system should be a member. It may be that some utilities are not aware that their local government and hence they are already members.



Takeaways and Next Steps

Overall, the utilities that responded to the survey are doing a good job with cybersecurity when their size is considered. Extrapolating to all PWS is difficult as the utilities that responded to the survey are probably the ones most interested in the topic and most progressive in their cybersecurity posture.

The following are some recommendations for advancing the cybersecurity of PWS given the survey results and risk-based considerations. The topics covered include ones in the survey as well as others that were not. They are grouped into priorities 1 – 3 with an overall target of making significant progress in all areas over the course of the next several years. Many of the cybersecurity measures can be implemented or organized by staff without cybersecurity or IT skills. They are indicated in the tables below with an "*".

Priority 1

Fortunately, the priority 1 activities, which are essential for baseline security, are generally lower cost and less demanding to complete. **It should be feasible for all municipal systems, and many of the non-municipal system, to establish these measures within 9 months**. In many cases they are likely already

implemented and may just need some degree of improvement. One possible strategy is to highlight a single measure each month with 1-2 page summaries that are essentially the same as MassDEP DWP cybersecurity posters with additional details and accompanying recorded short videos. Additionally, it would be useful to speak to some utilities that do not have a responsible cybersecurity leader identified to discuss possible solutions.

Priority	Cybersecurity Measures	Goal and Approach
1	Cybersecurity Leader and Budget *	**Goal**: Every utility needs to identify the leader who is responsible for advancing cybersecurity at their utility. Along with that commitment is the need to establish a Cybersecurity budget for next year if it does not already exist, regardless of how small it might be. **Approach**: Organize a focus group-type meeting of a handful of utilities to better understand constraints of assigning a cybersecurity leader and identify solutions.
1	Passwords * and Account Management	**Goal**: Every utility needs to require that all staff members use strong passwords and securely manage computer accounts by promptly disabling computer accounts of departing staff, limiting account access to what is required for a job description and having administrators use lower-level accounts for non-administrative activities. **Approach**: A 1-2 page summary and a short video.
1	Multi-factor Authentication	**Goal**: Every utility needs to activate multi-factor authentication for all external access to email systems, IT systems, OT systems and internal access to sensitive systems such as domain controllers. **Approach**: A 1-2 page summary and a short video.
1	Cybersecurity Awareness Training *	**Goal**: Every utility needs to establish cybersecurity awareness training for all staff. Short training sessions should happen at least quarterly and ideally monthly. Phishing drills are a common component. **Approach**: A 1-2 page summary and a short video.
1	Patching	**Goal**: Every utility needs to perform timely patching of essential servers and internet and e-mail exposed computers and devices as well devices used for segmentation. **Approach**: A 1-2 page summary and a short video.
1	Backups & Restoration Practice	**Goal**: Every utility needs to make regular backups that meet standards for resilience and to practice restoration.

		Approach: A 1-2 page summary and a short video.
1	Inventory of Software and Devices (IT and OT)	**Goal**: Every utility needs an inventory of IT and OT software and hardware so they can keep up with patching and be better able to response to a cybersecurity incident. **Approach**: A 1-2 page summary and a short video.
1	WaterISAC & MS-ISAC Memberships *	**Goal**: Ideally, every water utility in the Commonwealth would be a member of the WaterISAC, if they can afford it. The annual cost for small systems is $100 and climbs from there. Every municipal utility should be a member of the MS-ISAC, which is free and potentially provides some hands-on assistance during an incident. **Approach**: Prepare a 1-page summary that explains the benefits and costs of ISAC memberships. The document could also help municipal systems understand if they are already members. The MS-ISAC web site lists upwards of 120 cities and towns in Massachusetts that are members.

* – measures or activities that generally do not need cybersecurity or IT skills

Priority 2

Priority 2 measure are more demanding to implement than Priority 1 measures. They typically take more time to establish and, in some cases, require more technical skills to implement. Larger utilities may be able to incorporate many of these measures more quickly, if they have not already done so. Smaller utilities will be limited by staff and budget restrictions. A goal could be to have these measure in place for nearly all large utilities and most medium-sized utilities by the end of 2023.

Priority	Cybersecurity Measures	Goal and Approach
2	Manual Operations & Practice *	**Goal**: Every utility should understand to what degree they can run their process manually. Those that cannot operate manually need to identify where the shortcomings are and consider modifying their system to permit full manual control. All utilities should practice the various components of their manual operations in a carefully controlled way. **Approach**: A 1-2 page summary and a short video.
2	Incident Response Plan *	**Goal**: Every utility should have a cybersecurity incident response plan. This is both a documented plan and an arrangement for any supplement resources that might include an incident response firm on retainer or cybersecurity insurance that has response firms lined up.

		Approach: Planning a one-hour webinar on this topic and a draft incident response plan framework for mid-March.
2	Segmentation	**Goal**: Every utility should have their OT system protected from the internet and from their IT system with some form of segmentation. This requires technical skills and expenses. **Approach**: A 1-2 page summary and a short video.
2	Remote Access Hardening	**Goal**: Every utility should assess the remote access that they have to their IT and OT systems. If the applications are no longer supported, they should be replaced. Secure configuration options should be selected were possible. **Approach**: This assessment and potential updating activity may be possible by internal staff or may require hiring external expertise.
2	Policies and Procedures *	**Goal**: Writing and enforcing policies and procedures is a demanding activity. Every large and most medium and small utilities should have a set of basic policies and procedure that at least cover the Priority 1 measures. **Approach**: A 1-2 page summary and a short video.
2	End Point Detection software	**Goal**: All user computers should have anti-virus and malware detection software that is updated as appropriate. **Approach**: A 1-2 page summary and a short video.

* – measures or activities that generally do not need cybersecurity or IT skills

Priority 3

Priority 3 measures are important for good security and resilience during a cyber-attack. They can be extensive efforts and time-consuming projects. Some of them can be accomplished by in-house staff. One very valuable effort would be to survey willing utilities that installed cyber-physical safety systems to find out what they did so it can be shared with others.

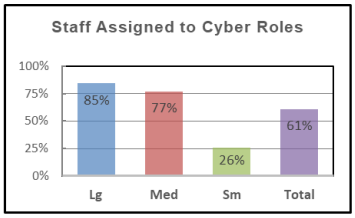
Priority	Cybersecurity Measures	Multi-Year Goal and Approach
3	Physical Security of IT and OT Assets *	**Goal**: Physical security is standard practice for water utilities. All utilities should provide additional protection for their computer and network assets. **Approach**: A 1-2 page summary and a short video.
3	End Point hardening	**Goal**: Every utility should do this, but it does require cybersecurity expertise and will vary slightly from system to system. This includes both onsite computers and remote mobile devices used for remote access. **Approach**: A 1-2 page summary and a short video.

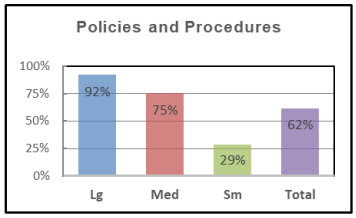
3	System Monitoring Independent of SCADA	**Goal**: This is a valuable resiliency resource for every utility but is a stretch to expect because of the extra expense to install and maintain. Very large system should be encouraged to do this as well as utilities that need it for manual operations. **Approach**: A 1-2 page summary and a short video.
3	ICS Monitoring	**Goal**: This is a currently a measure for larger utilities that have the resources to support it. **Approach**: The Water Sector Action Plan recently initiated by the National Security Council will provide advice to water utilities on how to approach and implement ICS monitoring.
3	Potential Cyber-Physical Damage Evaluation *	**Goal**: Every utility can do this. It can be a low-cost activity as existing staff and operators have excellent insight. **Approach**: A 1-2 page summary and a short video.
3	Cyber-Physical Safety System	**Goal**: Every large utility should look into the possibility of installing cyber-physical safety systems. **Approach**: There are a good number of utilities that have already done this, and it would be valuable to understand their solutions in order to share with others. Prepare a 1-2 page summary along with a short video.

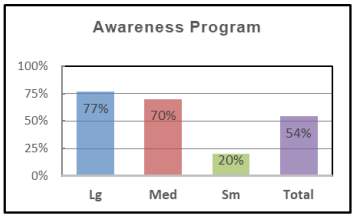
* – measures or activities that generally do not need cybersecurity or IT skills

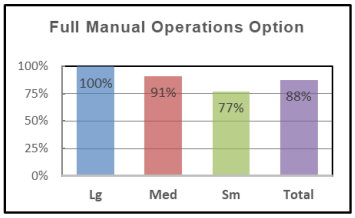
Overview of Survey Results by Utility Size - Dec. 2021

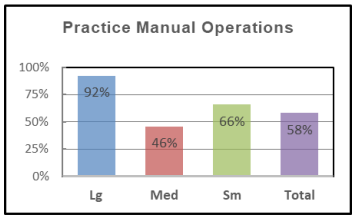
A total of **105 utilities responded** to the survey. Most were Community systems, with 12 Transient Non-Community and 9 Non-Transient Non-Community systems. **13 large utilities** (> 50,000 people) responded out of 38 in the Commonwealth, 57 **medium utilities** (<= 50,000 and > 3,300) out of 259, and **35 small utilities** (<= 3,300) out of approximately 1,300.

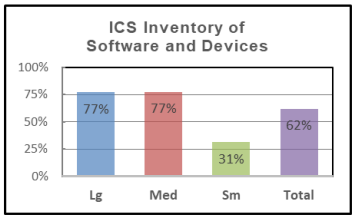


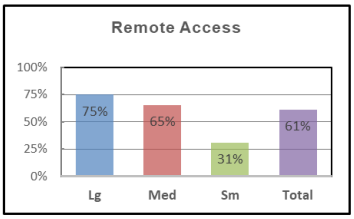


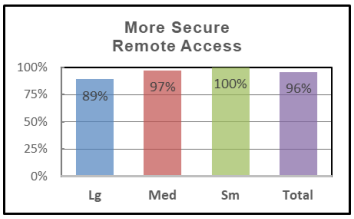


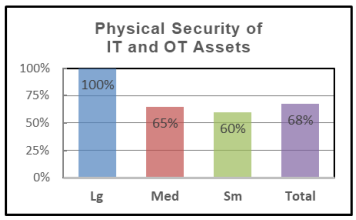


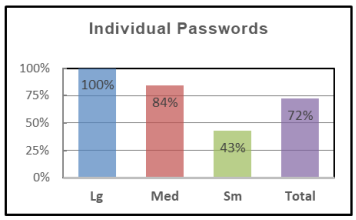


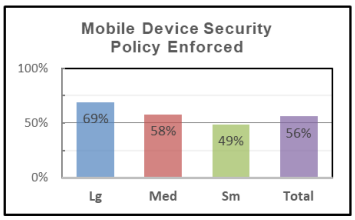


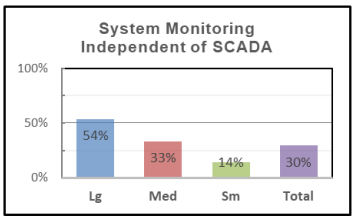


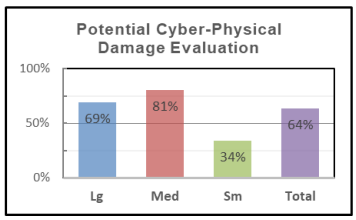


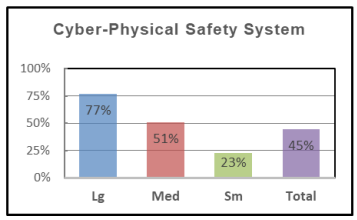


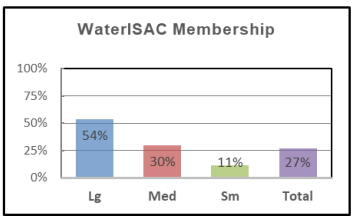


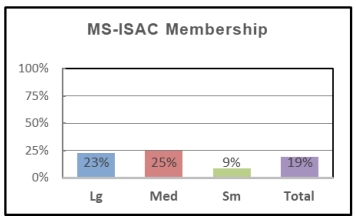












Utility Size Legend: **Large** > 50,000 people **Medium** > 3,300 and <= 50,000 people **Small** <= 3,300 people

Note, the "More Secure Remote Access" graph (second row on the far right) represents the degree to which utilities that require and use remote access for their SCADA system are using methods that are considered more secure.

No Restriction on Distribution-
Contains No Sensitive Information

Survey Questions

1. Does the system have a security lead that oversees IT and OT cybersecurity-related duties, with a manager that is responsible for the outcomes?

2. Do you have formal cybersecurity policies and procedures?

3. Does the system have an ongoing employee cyber security awareness training program?

4. If your primary process control system (SCADA) goes down because it is attacked, or for any other reason, can all of your treatment and distribution processes be operated “manually”?

5. Do you practice running all or part of the system “manually”?

6. If yes, how often

7. Does your system keep an inventory of control system software and networked devices?

8. Do you require remote access to your SCADA system for operations or maintenance?

9. If yes, do you protect the remote access by one of the following or other comparable methods? (e.g., multifactor authentication, jump server, virtual private network or VPN, etc.)

10. Does your system prevent unauthorized access to IT and OT systems through physical security measures (e.g., locked server rooms and cabinets, alarms)?

11. Does your system require individual employee passwords for workstations?

12. Does your system enforce policies for the security of mobile devices?

13. Do you have a remote monitoring system that is independent of the SCADA system? (e.g. data loggers)

14. Have you evaluated your water treatment and distribution process for critical systems or equipment that might be vulnerable to damage from a cyber-attack?

15. Are there independent cyber-physical safety systems that you could implement to protect those vulnerable critical systems?

16. Is the system a member of WaterISAC?

17. Is the system a member of MS-ISAC?