CYBER RISKS & RESOURCES
FOR THE WATER AND WASTEWATER SYSTEMS SECTOR

The Water and Wastewater Systems Sector provides essential services that support the operation of all U.S. critical infrastructure. Water and wastewater facilities rely on information technology (IT) and operational technology (OT) systems to operate, and a compromise of these systems could lead to disruptions of service and significant cascading impacts throughout U.S. critical infrastructure. The Cybersecurity and Infrastructure Security Agency (CISA) developed this infographic to highlight potential cyber risks to the management of wastewater and provide available resources to support proper cybersecurity and resilience.

RISKS TO THE MANAGE WASTEWATER NATIONAL CRITICAL FUNCTION

Information Technology (IT) Systems

1 DATA

Malicious actors may attempt to access IT systems to steal sensitive data, disable network components, and move laterally within the network to access other more sensitive systems.

2 RANSOMWARE

Ransomware attacks can disrupt operations within a facility until systems are restored. While disruptions in office-based systems are most common, it is possible for ransomware to also infect connected Operational Technology (OT) systems, particularly if there is not adequate segmentation between IT and OT systems.

IT/OT Convergence

3 NETWORK SEGMENTATION

Malicious actors may use IT networks as a vector to target non-segmented OT networks and systems. Proper network segmentation is the most effective way to prevent cyber-attacks against OT networks.

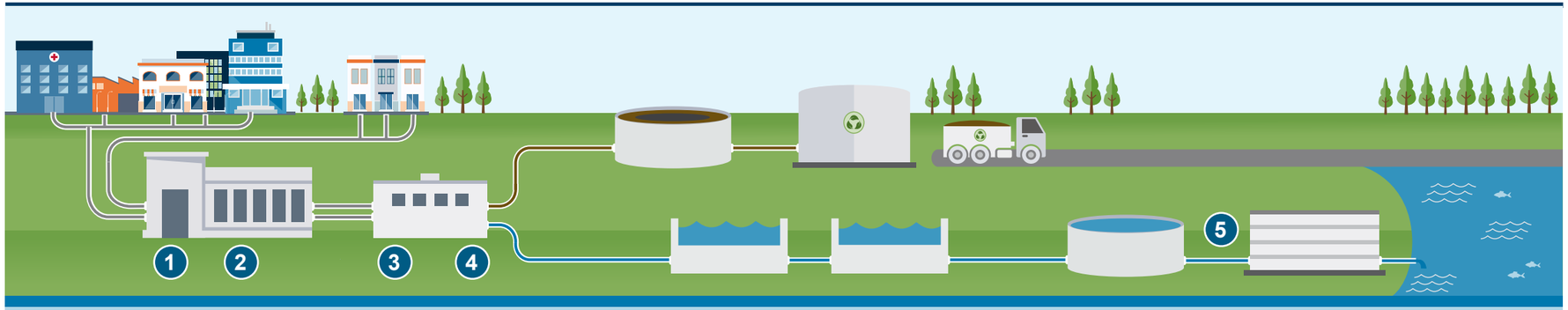
Operational Technology (OT)

4 NETWORK COMPLEXITY

Wastewater management OT networks may contain hundreds of diverse components that can be difficult to properly map and update. This complexity may lead to operators not having full visibility into their networks and may contribute to misconfigurations and continued usage of components that are not included in a utility's network mapping.

5 SYSTEM MAINTENANCE

Improperly maintained custom and Commercial off the Shelf (COTS) components, particularly those that have not been kept up to date on security patches or are operating beyond end-of-life, can leave OT systems vulnerable to attack. Managed Service Providers (MSP) may be used within critical infrastructure to support both IT and OT networks, and if compromised, could provide adversaries with remote access into customers' OT systems. A successful exploitation of an OT system can provide attackers with a direct means of manipulating systems that support the management of wastewater systems.



Data

Ransomware

Network Segmentation

Network Complexity

System Maintenance

1 2 3 4 5

IT SYSTEMS

Implementing cyber hygiene and best practices within IT networks can protect wastewater management systems from cyber attacks such as ransomware and data theft, and reduce the risk of lateral movement within systems or networks.

IT/OT CONVERGENCE

Properly segmenting IT/OT systems, and ensuring that no part of OT systems connect directly to the internet, can greatly reduce the possibility of a successful attack upon ICS/SCADA systems that support the manage wastewater function.

OT SYSTEMS

System owners should ensure that OT systems that help wastewater systems control valves and pumps and monitoring are properly protected through patching and proper network mapping. Human machine interfaces, through which operators typically control OT systems, should be a priority for securing.

RESOURCES

AVAILABLE RESOURCES INCLUDE: CISA's **Cyber Resource Hub** provides a range of free, immediately available cybersecurity resources. CISA's **Cyber Essentials Toolkit** for non-technical leadership. **Securing Networking Devices** provides guidance on Segmenting and Segregating Networks. **Stopransomware.gov** contains best practices for preventing or responding to ransomware. The **Industrial Control Systems Joint Working Group (ICS-JWG)** has links to trainings and resources related to the securing and safe operation of ICS systems. CISA also provides no-cost **cybersecurity assessments.** The **WaterISAC** provides wastewater managers with cyber hygiene and water security resources. The **AWWA's Security Guidance and Tool** supports the sector in implementing the NIST Cybersecurity Framework and use of Cybersecurity Guidance and Assessment Tool.