CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY
OCTOBER 2021

CYBER RISKS & RESOURCES FOR THE WATER AND WASTEWATER SYSTEMS SECTOR

The Cybersecurity and Infrastructure Security Agency (CISA) developed this infographic to highlight cyber risks and provide available resources to support the Water and Wastewater Systems Sector. The Federal Government released **Joint Cybersecurity Advisory AA21-287A** on October 14, 2021 in response to unauthorized access of Supervisory Control and Data Acquisition (SCADA) systems at U.S. drinking water treatment facilities. Cyber criminals have been observed targeting desktop sharing applications, which despite having legitimate uses, can also be exploited through malicious actors' use of social engineering tactics and other illicit measures. Computer networks running operating systems with end-of-life status also pose significant risks that malicious actors will gain unauthorized access to systems.

RISKS TO THE SUPPLY WATER NATIONAL CRITICAL FUNCTION

Operational Technology (OT)

1 NETWORK COMPLEXITY

Water 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.

2 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 water 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.

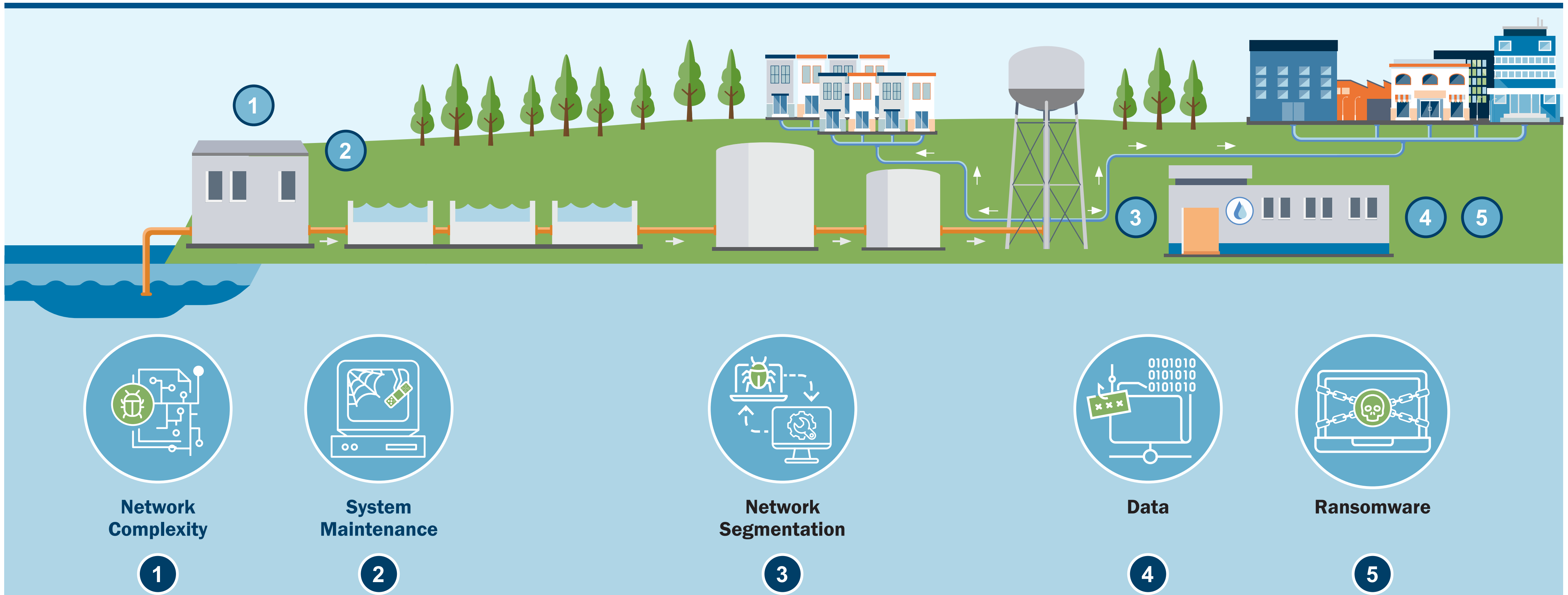
Information Technology (IT) Systems

4 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. Malicious actors may also attempt to use stolen information to move laterally within the network and access other more sensitive areas.

5 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 OT systems, particularly if there is not adequate segmentation between IT and OT systems.



OT SYSTEMS

System owners should ensure that OT systems that help water 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.

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 Industrial Control Systems (ICS)/SCADA systems that support the supply water function.

IT SYSTEMS

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

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** produces physical and cyber threat alerts and best practices specifically for the water and wastewater sector. The **AWWA's Security Guidance and Tool** supports the sector in implementing the NIST Cybersecurity Framework and use of Cybersecurity Guidance and Assessment Tool.