Cybersecurity Resource Guide

October 2016

In recognition of the 13th Annual National Cyber Security Awareness Month, WaterISAC has updated this Cybersecurity Resource Guide. The guide contains actionable and informative resources to help water and wastewater utilities and the government agencies that support them plan for cyber incidents, mitigate risks, resolve vulnerabilities, and identify threats. All of the resources below are available in the WaterISAC portal. For the resources only available to Pro members, consider a free three-month Pro membership trial.

Contents:

Introduction

As with any critical enterprise or corporation, water and wastewater utilities must evaluate and mitigate their risks from malicious cyber attacks. Hackers range from cyber criminals, politically motivated activists and terrorists to entire networks sponsored by nation states and international political, criminal and terrorist organizations. The theft of customer data and resulting loss of customer confidence can result in damages ranging from moderate inconvenience to sizable expenses related to business interruptions and lawsuits. Sophisticated hackers can also infiltrate SCADA or industrial control systems (ICS) and potentially create both health and economic damages through the interruption of vital water treatment and distribution processes.

To help water and wastewater utilities address these threats, WaterISAC provides members with a rich clearinghouse of information about cybersecurity, not to mention physical security and emergency response.

If you are not a member of WaterISAC Basic or Pro, consider joining to access these resources. WaterISAC Basic memberships are free, and WaterISAC offers free three-month trial WaterISAC Pro memberships to new members.

Visit www.waterisac.org/join and explore WaterISAC.

Please contact WaterISAC with any questions or comments at info@waterisac.org or 866-H2O-ISAC.

Threat Information Sources

An important part of promoting and safeguarding your organization's cybersecurity is being aware of the kinds of threats that exist and actual attacks being conducted against critical infrastructure. This information comes from many sources, and WaterISAC collects, filters and disseminates this data to provide members with a focused and accurate depiction of current and emerging cyber threat environments.

The WaterISAC portal is a library of hundreds of cybersecurity resources. Posted information can be viewed chronologically or by using the portal's search feature. Sources of WaterISAC's cybersecurity threat information include federal departments and agencies, such as the U.S. Department of Homeland Security (DHS), in particular the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) and the U.S. Computer Emergency Readiness Team (US-CERT), as well as the Federal Bureau of Investigation (FBI) and other agencies.

In addition to its government partners, WaterISAC partners with other ISACs and private cybersecurity firms and looks to software and hardware vendors, academic institutions and

think tanks, industry associations, not to mention water and wastewater utilities, for information on cybersecurity incidents and threats.

WaterISAC also conducts monthly Water Sector Cyber Threat Briefings with ICS-CERT and experts from FireEye iSIGHT. All past briefings are available to WaterISAC Pro members on the WaterISAC portal.

NIST Cybersecurity Framework

To help businesses and organizations voluntarily improve cybersecurity, the President signed Executive Order (EO) 13636: Improving Critical Infrastructure Cybersecurity, in February 2013. The most relevant section of the EO for the water and wastewater sector concerns the development of the Cybersecurity Framework by the National Institute of Standards and Technology (NIST) to help critical infrastructure sectors and organizations reduce and manage their cyber risks.

To support the water and wastewater sector's implementation of the NIST Cybersecurity Framework, the American Water Works Association (AWWA) created its Cybersecurity Guidance and Tool. WaterISAC recommends water and wastewater personnel and third-party support responsible for IT and industrial control systems to download and use the guidance and tool. Both the framework and the AWWA products contain recommended risk reduction measures and link the user to standards, guidelines and practices to implement those measures.

AWWA Cybersecurity Guidance and Tool

AWWA's cybersecurity guidance – *Process Control System Security Guidance for the Water Sector* – provides water and wastewater utilities with recommended courses of action to reduce vulnerabilities to cyber attacks. The controls are in direct alignment with the NIST Cybersecurity Framework and principles in *ANSI/AWWA G430: Security Practices for Operations and Management*. The guidance is organized to focus utility managers and boards on the practices essential to supporting an effective cybersecurity risk management program.

The AWWA guidance is supported by a use-case tool that generates a prioritized list of recommended controls based on the specific characteristics of a utility. The user selects the applicable use-case (i.e., remotely operate pump station with control) and is provided with a prioritized list of controls to compare with their as-built conditions. The use-case tool emphasizes actionable recommendations with the highest priority assigned to those controls expected to provide the most immediate impact on risk mitigation.

This resource has been recognized as the water sector's voluntary approach to implementing the NIST Cybersecurity Framework by the Water Sector Coordinating Council, U.S. EPA and DHS.

Assessment Tools and Services

WaterISAC encourages water and wastewater systems to assess their vulnerabilities to cyber intrusion. In addition to the NIST and AWWA products, the Department of Homeland Security offers several free tools to help utilities accomplish this. Utilities can use them on their own or schedule free on-site assessments by ICS-CERT. Refer to the ICS-CERT assessments page for details.

Cybersecurity Evaluation Tool

The Cybersecurity Evaluation Tool (CSET) is a desktop application that can be utilized by utility employees with or without the assistance of ICS-CERT personnel. Developed under the direction of ICS-CERT, CSET guides users through a step-by-step process to assess their control system and information technology network security practices against recognized industry standards. The output from CSET is a prioritized list of recommendations for improving the cybersecurity posture of the organization's enterprise and industrial control systems. Each recommendation is linked to a set of actions that can be applied to enhance cybersecurity controls. The tool is updated periodically to include additional features and evaluation standards.

Design Architecture Review & Network Architecture Verification and Validation

ICS-CERT also provides on-site visits to conduct the Design Architecture Review (DAR) and the Network Architecture Verification and Validation (NAVV). Both of these services feature a "deep-dive" into an organization's system architecture. The DAR is a 2-3 day review that examines data egress and ingress pathways and communications channels and ensures appropriate network perimeter defenses are in place. Among other features, a NAVV helps to verify device-to-device communications and validates data flow within a system.

For more information, download the Control Systems Architecture Analysis Services Fact Sheet. To schedule an on-site CSET assessment, DAR or NAVV, email cset@dhs.gov.

Cyber Resilience Review

Designed as either a self-assessment or as an on-site assessment conducted by DHS cybersecurity professionals, the Cyber Resilience Review (CRR) is a no-cost, voluntary, non-technical assessment to evaluate an organization's operational resilience and cybersecurity. The CRR assesses enterprise programs and practices across a range of ten domains, including risk management, incident management and service continuity. To request an onsite CRR, email CSE@hq.dhs.gov.

Confidentiality of Critical Infrastructure Information

All information collected during these assessments is protected under DHS's Protected Critical Infrastructure Information (PCII) program. PCII-protected information is not subject to federal, state, local or tribal public disclosure laws and may not be used in regulatory actions or civil litigation.

Other Guides and Resources

Visit the 2016 Cyber Security Awareness Month websites of the Department of Homeland Security and the MS-ISAC for links to a range of educational resources.

Best Practices

WaterISAC's 10 Basic Cybersecurity Measures to Reduce Exploitable Weaknesses and Attacks was developed in conjunction with ICS-CERT, the MS-ISAC, and the Information Technology ISAC. The ten overarching recommendations identify basic steps that can help water and wastewater utilities reduce their vulnerabilities and defend against avoidable data breaches and cyber attacks. Each of the recommendations included in this document contains links to corresponding technical resources.

Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies, updated by DHS in September 2016, advocates a holistic approach, using specific countermeasures to create multiple layers of defenses against cybersecurity threats and vulnerabilities. This approach is often referred to as "defense-in-depth." While these strategies are not new, the recent convergence of IT and ICS systems and high-profile intrusions have highlighted the potential risk to ICS. The guide covers risk management, asset inventory, physical security, network architectures, monitoring, security attacks, a proactive security model, five key countermeasures and security standards, along with security tools and services.

Seven Strategies to Effectively Defend Industrial Control Systems, published by DHS along with the U.S. Department of Justice and the National Security Agency at the end of 2015, illustrates seven strategies to defend ICS: implement application whitelisting; ensure proper configuration and patch management; reduce your attack surface area; build a defendable environment; manage authentication; monitor and respond, and implement secure remote access. According to the document, 98% of incidents reported to ICS-CERT from 2014 to 2015 could have been prevented with these steps. The remaining 2% could have been identified with increased monitoring and robust incident response.

ICS-CERT also published its guidelines for implementing application whitelisting (AWL) as a cybersecurity measure in ICS. This document serves as an appendix to the *Seven Steps to Defend Industrial Control Systems* to provide additional conceptual-level guidance on AWL implementation. AWL can be used to detect and prevent attempted execution of malware uploaded by adversaries. ICS-CERT encourages operators to work with vendors to calibrate AWL

deployments. As noted in a *NIST Guide to Industrial Control Systems Security (SP 800-82)*, updated in May 2015, provides an overview of industrial control systems and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks. These standards are also covered in the ICS-CERT's CSET assessment.

Vulnerabilities, Dependencies and Consequences

DHS's Office of Cyber and Infrastructure Analysis released the report *Analysis of Water and Wastewater Sector Cyber-Physical Risk in Smart Cities* to address how the adoption of and increased reliance on smart technologies may create or increase risk for cities. This report focuses on the water and wastewater sector, as well as the energy and transportation sectors. It provides an overview of smart technologies as they are used by the sectors, describes vulnerabilities that may arise, and addresses opportunities for DHS to provide assistance to reduce risks.

Published in August 2016, ICS-CERT's *Industrial Control Systems Assessment Summary Report* for fiscal year 2015 covers cybersecurity and resilience for critical infrastructure facilities, including drinking water and wastewater utilities. Among the findings, the top six categories of security practices accounted for 36% of all weaknesses found in assessments. These involved boundary protections, least functionality, authentication management, identification and authentication, least privilege, and allocation of resources. These practices were mapped against requirements listed in *NIST Special Publication 800-53*.

Organizations looking to implement cyber threat detection and mitigation on their networks should become familiar with the Cyber Kill Chain model. Multiple variations of cyber kill chains exist. The one used in conjunction with STIX information standards by DHS and other agencies is the Lockheed Martin cyber kill chain. WaterISAC's July 2016 webcast discusses each phase of the cyber kill chain and how it is used in network defense to stop attacks and perform analysis.

Data Breaches and Compromised User Credentials

The frequency and volume of data breaches have grown in recent years. Attackers often search for users' credentials to gain access to data. An organization's data can be targeted by cyber criminals for financial gain and advanced persistent threats for espionage and potential sabotage.

The California Attorney General's *Data Breach Report for 2016* provides recommendations for 20 security controls to protect data. According to the report, nearly three in five Californians were victims of data breaches from 2012 to 2015. While data breach is more frequently associated with the healthcare and retail sectors, any organization with a database of customer information is a potential target.

Attackers can also leverage compromised user credentials to gain access across an organization's networks as observed in the Ukraine power grid outages of December 2015. ICS-CERT and other trusted partners have published summaries of these attacks along with recommended mitigation steps.

On an administrative level, recommendations for protecting user credentials across common attack scenarios are covered in a white paper by cybersecurity firm Praetorian, titled *How to Dramatically Improve Corporate IT Security without Spending Millions*.

At the C-Suite level, The Economist and Oracle published a study titled *The C-Suite, the Board and Cyber-Defence* that shows how certain firms are able to consistently reduce data breaches across all major forms of cyber attacks. Also, the cybersecurity firm F-Secure shared lessons learned from data breaches and how they impact leadership. Among the findings, a major security incident can divert leadership's focus from daily business goals for months.

Following the September 2016 disclosure of 500 million comprised Yahoo user accounts dating back to 2014, the U.S. Federal Trade Commission released its *Data Breach Recovery and Prevention Video*.

When a data breach does occur, AT&T's *The CEO's Guide to Cyberbreach Response* describes well prepared versus less prepared organizations, the core components of an incident response plan, scenarios to include in a playbook, how to mitigate ransomware, how to communicate a breach, and lists additional resources. In addition, IBM published a guide titled *Top 10 Mistakes to Avoid in a Computer Security Incident Response Plan*. IBM's guide also includes dos and don'ts when a security incident is declared.

Social Engineering Attacks

According to multiple government and open source reporting, users remain highly susceptible to social engineering scams, especially ransomware attacks and business email compromise scams. These types of social engineering attacks have dramatically increased over the past year and have affected multiple utilities.

In June 2016, multiple U.S. Government entities released an interagency technical guidance titled *How to Protect Your Networks from Ransomware* along with a CEO Ransomware handout. In August 2016, multiple cybersecurity firms published the white paper *Best Practices for Dealing with Phishing and Ransomware*.

WaterISAC encourages users to remain aware of social engineering and phishing attacks that attempt to steal account credentials for data breaches or other attacks. Users can review US-CERT's Security Tip *How to Avoid Social Engineering Scams (ST04-014)* and the DHS guide, *Deception: The Art of Social Engineering*.

Distributed Denial-of-Service Attacks

The Communications-Information Sharing and Analysis Center (C-ISAC) published the August 2016 white paper *Distributed Denial-of-Service (DDoS) Attacks Common Practices*. This paper covers different types of DDoS attacks, a basic understanding of how they are delivered, the impact to network bandwidth, and common best practices for minimizing and protecting from them.

Similarly, cybersecurity firm Impervia published the *Network Ops DDoS Playbook* in June 2016 that covers how to choose a protection strategy, maximize preparedness, respond to an attack, and conduct post-attack steps. The Multistate Information Sharing and Analysis Center (MS-ISAC) also published a technical white paper, *Guide to DDoS Attacks*.

Advanced Persistent Threats

The Institute for Critical Infrastructure Technology (ICIT) published a report on hacking incidents against the energy sector along with some of the advanced persistent threat (APT) groups and nation-states who have conducted them. *The Energy Sector Hacker Report* (August 2016) covers tactics, techniques, and procedures used in these attacks and the types of threat actors. While the focus is on the energy sector, APT groups have been known to target other sectors and interests over time. ICIT also released an updated primer on APT groups, *Know Your Enemies*.

Insider Threats

In May 2016, Experian and Ponemon Institute published the results of a study titled *Managing Insider Risk Through Training & Culture*. The researchers provide recommendations to make training more engaging and easier to retain. To change the culture, employees should be provided with incentives and senior executives should set the example by participating.

The Pennsylvania Criminal Intelligence Center (PaCIC) released a report on insider threats against critical infrastructure organizations in December 2015. Insider threats can be difficult to detect due to approved access and knowledge of business operations. A number of suspicious behaviors and background information is available in the PaCIC report *The Insider Threat*.

STOP. THINK. CONNECT.

For more basic tips and resources for staying safe online, visit STOP. THINK. CONNECT. and the National Cyber Security Alliance. Also, visit the Anti-Phishing Work Group to learn about protecting yourself from phishing.

ICS Cybersecurity Awareness for Executives

ICS-CERT published its guide titled *ICS Cybersecurity for the C-Level*, which covers key risk management concepts and questions executives should ask about ICS attacks and long-term threats. The guide includes ICS-CERT assessment resources and assistance.

DHS Critical Infrastructure Cyber Community Voluntary Program

Critical Infrastructure Cyber Community (C3) was created by DHS to help industry understand the NIST Framework and other cyber risk management efforts. C3 currently focuses on DHS tools and services, but is expected to expand to include others. Visit the C3 Voluntary Program US-CERT Gateway to download the C3 Outreach and Messaging Kit. In it are fact sheets on "5 Questions CEOs Should Ask About Cyber Risks" and "Key Cyber Risk Management Concepts," plus information about the voluntary program.

Education and Training

There are numerous courses and education opportunities available, many of which are offered at no cost, for the public and private sector to gain a better understanding of information systems and of the issues that potentially threaten these systems.

WaterISAC Events Webpage

WaterISAC frequently posts information on upcoming training opportunities on its Events page. WaterISAC's twice-weekly Security & Resilience Update also lists webinars, instructor-led courses and conferences.

ICS-CERT

DHS ICS-CERT provides online, self-run classes as well as instructor-led courses. Courses are presented at regional venues in various locations throughout the year. These courses range from introductory to technical level cybersecurity for industrial control systems. Refer to the ICS-CERT calendar for a schedule of these training options.

Other Providers

The CERT Insider Threat Center has created an Insider Threat Program Manager (ITPM) Certificate Program. The program is designed to assist insider threat program managers with developing a formal insider threat program. It covers areas such as insider threat planning, identification of internal and external stakeholders, components of an insider threat program, insider threat team development, strategies for effective communication of the program, and how to effectively implement and operate the program within the organization.

The Texas A&M Engineering Extension Service, better known as TEEX, provides internationally recognized training on emergency response and homeland security, including cybersecurity.

Other sources of training include water and wastewater associations and the Rural Community Assistance Program.

Industry associations such as ISACA (formerly the Information Systems Audit and Control Association) and the Information Systems Security Association (ISSA) also offer cybersecurity education and training opportunities for members. ISACA has online training courses, conferences, dedicated training weeks, on-site training, and education curriculums. ISSA hosts international conferences, local chapter meetings, and seminars with training.

Cybersecurity Insurance

Cybersecurity insurance to mitigate losses from a variety of cyber incidents is becoming more widely available. Many corporate liability policies do not cover cyber-related liabilities, requiring the purchase of a separate cybersecurity insurance policy. Such policies cover many cyber-related expenses, depending on the type of policy purchased.

The Financial Services Sector Coordinating Council (FSSCC) has published the *Purchaser's Guide to Cyber Insurance Products*. The guide is intended to provide resources and advice, particularly to small and medium-sized organizations, that are considering cyber insurance. The insurance industry has responded to cyber risks by offering a variety of coverages for liability and remediation costs such as customer notifications and forensic investigations. The guide includes three main reasons for considering cyber insurance and how to evaluate plans to cover them.

Insurance analytics company Advisen published the white paper *The Evolving Risks to Small Businesses and Their Data*, which takes into account that cyber attacks on small businesses can take a more significant toll compared to large businesses. The paper examines why small businesses are a target, types of attacks most likely to affect them, and tips and services that can help against cyber crime. Considering small businesses account for 99% of all U.S. businesses, a number of cyber insurers, brokers, and cybersecurity vendors are offering solutions and advice.

Meanwhile, the SANS Institute has identified gaps between cyber insurance and cybersecurity communities that should be resolved to reduce the risk of financial losses.

Who to Call if You've Been Hacked

If you believe your organization has been targeted in a cyber attack, please contact authorities and notify WaterISAC. At DHS, ICS-CERT and US-CERT both work to mitigate cybersecurity incidents experienced by public and private sector partners.

ICS-CERT provides onsite incident response and forensic analysis to owners and operators of critical infrastructure. To report an incident to ICS-CERT, send an email to ics-cert@hq.dhs.gov or call (877) 776-7585.

US-CERT provides both remote and onsite response support to Federal Executive Branch civilian networks and the private sector. US-CERT can be contacted by emailing soc@us-cert.gov or by calling (888) 282-0870.

Depending on the situation, WaterISAC can help members get in contact with authorities, raise issues to their appropriate level of attention, leverage the expertise of its vast and knowledgeable member community and provide recommendations for mitigating actions. All reports are confidential and are only shared with the permission of the reporting entity.

WaterISAC can be reached by email at analyst@waterisac.org, by phone at (866) H2O-ISAC, or by completing the incident reporting form at https://www.waterisac.org/report-incident.

If you wish to report a cybercrime to the FBI, contact your local FBI office.