WATER ISAC

15 Cybersecurity Fundamentals for Water and Wastewater Utilities

Best Practices to Reduce Exploitable Weaknesses and Attacks

2019

waterisac.org/fundamentals

15 Cybersecurity Fundamentals for Water and Wastewater Utilities

Water Information Sharing and Analysis Center (WaterISAC)
1620 I Street, NW, Suite 500
Washington, DC 20006
www.waterisac.org
866-H2O-ISAC
support@waterisac.org

About WaterISAC

The mission of the Water Information Sharing and Analysis Center, better known as WaterISAC, is to enhance the security of water and wastewater utilities by providing information and tools for preventing, detecting, responding to, and recovering from all hazards.

WaterISAC is a non-profit organization created in 2002 by and for the water and wastewater sector. It is governed by a board of managers comprising water and wastewater utility managers and a state drinking water agency administrator who are appointed by the American Water Works Association, the Association of Metropolitan Water Agencies, the Association of State Drinking Water Administrators, the National Association of Clean Water Agencies, the National Association of Water Companies, the National Rural Water Association, the Water Environment Association and the Water Research Foundation.

Member organizations include drinking water and wastewater utilities, local, state and federal government agencies, industry organizations and private firms that support water and wastewater utilities.

WaterISAC is the only all-threats security information source for the water and wastewater sector. It is the most comprehensive and targeted single point source for data, facts and analysis on water security and threats. WaterISAC also provides analysis and resources to support response, mitigation and resilience initiatives.

WaterISAC delivers timely, actionable information you can put to use right away to **Supercharge Your Security**.

Learn more and join WaterISAC at waterisac.org/membership.

For more information about WaterISAC, contact:

Michael Arceneaux
Managing Director
202-331-0479
arceneaux@waterisac.org

Preface

The original version of this guide, “10 Basic Cybersecurity Measures to Reduce Exploitable Weaknesses and Attacks,” appeared in 2012 and was updated in 2014 and 2016. This new version has been significantly reorganized and revamped and it contains the latest information. Therefore, the guide has the new name it appears with today.

The guide is intended to provide an overview of cybersecurity measures, not to be an exhaustive resource or a step-by-step guide. Hyperlinked resources produced by government and private sources accompany each measure for deeper exploration.

Acknowledgements

WaterISAC thanks Jennifer Lyn Walker, WaterISAC cybersecurity risk analyst, for leading the development of this guide. WaterISAC also gives special thanks to Andrew Hildick-Smith of the Massachusetts Water Resources Authority for his advice and his very substantial contributions to the guide's content.

WaterISAC also thanks its members, whose dues made this guide possible.

Table of Contents

Introduction

Water and wastewater utilities provide critical lifeline services to their communities and their regions. Safe water and clean water are essential for public health, ecosystem protection and economic strength. Supporting these important functions requires secure information technology (IT) and operational technology (OT).

Yet, our sector's IT and OT networks continue to face an onslaught of threats from cyber criminals and nation-states, hacktivists and others. Cyber criminals' attacks, both indiscriminate and targeted, are designed to steal or extract money and collect sensitive personal information, which in turn can be sold to the highest bidder. Nation-states – primarily Russia, China, North Korea and Iran – have demonstrated the desire and ability to infiltrate IT and OT systems and, in the case of the energy and manufacturing sectors in other countries, to disrupt operations.

"Moscow is now staging cyberattack assets to allow it to disrupt or damage U.S. civilian and military infrastructure during a crisis, and poses a significant cyber influence threat," says Dan Coats, Director of National Intelligence.

IT and OT compromises can have great impact on a utility. These include the loss of staff productivity and the cost of rectifying an IT or OT compromise, as well as reputational damage that can result from allowing the theft of customer data. Worse, potential operational disruptions could jeopardize public health and environmental protection.

Although many water and wastewater utilities have invested the necessary time and resources in cybersecurity, more progress is necessary on the part of the sector to secure IT and OT systems. This guide is intended to show a path toward that goal.

The guide will also be helpful to utilities preparing risk and resilience assessments required by America's Water Infrastructure Act, or AWIA. The 15 fundamentals discussed here will also be especially useful for informing emergency response plans because AWIA requires those plans to address mitigation and resilience options.

John P. Sullivan, PE, BCEE
Chairman

Diane VanDe Hei
Executive Director

Report Incidents and Suspicious Activity to WaterISAC and Authorities

"It takes a community to protect a community." That is the underlying theme of the Department of Homeland Security's "If You See Something, Say Something" program. It is also the foundation of information sharing and it is what motivates WaterISAC's mission to help protect the security of our members and the water and wastewater sector at large.

WaterISAC urges utilities and others sector stakeholders to report incidents and suspicious activity to our analysts. Reporting incidents and suspicious activity helps strengthen sector resilience, because it allows WaterISAC to identify threats and vulnerabilities and to warn other members and partners. The information you share also helps WaterISAC shape products and services, including webinars and reports, that can help utilities stay safe and secure.

WaterISAC maintains confidentiality of the information provided by submitters. If WaterISAC wishes to share your incident in an analysis or other product, we would first secure your express permission to do so, then would anonymize the information you have shared. As a private non-profit, WaterISAC is not subject to public records law, further preserving the security of your report.

In some cases it may necessary or preferable to also report your incident or suspected incident to federal authorities, especially if you intend to seek help with an investigation or recovery. Crimes should always be reported to the appropriate authorities.

How do I make a report?
You can file reports of incidents and suspicious activity in three ways:

1. By filing a confidential report at www.waterisac.org/report -incident.
2. By emailing analyst@waterisac.org.
3. By calling our analyst desk at 866-H2O-ISAC.

What do I report?
WaterISAC seeks reports of both cyber and physical incidents, as well as suspicious activity.

Cybersecurity Incidents

Cybersecurity incidents are cyber attacks or compromises of your enterprise IT system or your industrial control system. These events could be:

- Successful ransomware attacks or close calls.
- Successful installations of malware that had or may have had an impact on the utility's ability to conduct business and operations.
- Phishing campaigns, including successful or attempted spear phishing of executives, executive assistants, SCADA engineers, IT administrators or other privileged users.

- Successful or attempted business email compromise incidents, including account takeover or impersonation of executives.
- Data thefts.
- Social engineering attempts to gather sensitive information from personnel.

Physical Security Incidents

Reportable physical security incidents include those that are intended to cause any of the following:

- Bodily harm to employees or customers.
- Public health impacts.
- Significant harm to the environment.
- Impacts to the operations of your utility.
- Financial losses to your organization of $10,000 or more (per instance.)

Specific examples of these types of incidents include:

- Intentional water supply or wastewater contamination.
- Sabotage/tampering.
- Theft.
- Assault.
- Surveillance or suspicious questioning.
- Threats.

What happens next?
Once you alert us to the incident or suspicious activity, we will follow up with you for more information. Then we will ask whether we can use the information in WaterISAC reports. If the answer is yes, we will anonymize the information you shared by removing any details that would attribute the incident to you or your utility. The information you share is stored in a protected database. The anonymized information will be used to inform WaterISAC's "Threat Analysis Report," which is produced twice each year for members, and perhaps other reports.

Federal and Other Reporting Mechanisms

United States

Department of Homeland Security National Cybersecurity and Communications Integration Center (NCCIC). Report incidents to NCCIC by emailing NCCICCUSTOMERSERVICE@hq.dhs.gov or by calling 888-282-0870. You may also contact WaterISAC for an introduction to NCCIC staff. DHS can protect sensitive information that is shared with its teams, if requested.

NCCIC's Hunt and Incident Response Team provides onsite incident response free of charge to organizations that require immediate investigation and resolution of cyber compromises.

Federal Bureau of Investigation (FBI). The FBI encourages victims of internet crimes to contact an FBI field office. Crime complaints can also be made to the bureau's Internet Crime Complaint Center (IC3) at www.ic3.gov.

MS-ISAC and E-ISAC. Members of the Multi-State ISAC and the Electricity ISAC should report incidents through established channels.

Fusion Centers. State Fusion Centers are another possible reporting option. Fusion centers are effective at appropriately sharing information and have strong relationships with DHS and other organizations.

Australia

Utilities in Australia may report incidents to CERT Australia, which is a division of the Australian Cyber Security Centre, by calling 1300-CYBER1 or emailing info@cert.gov.au.

Canada

Utilities in Canada may report incidents to the Canadian Cyber Incident Response Centre by calling 1-833-CYBER-88 or by emailing contact@cyber.gc.ca.

1. Perform Asset Inventories

Since you cannot protect or secure what you do not know you have, identifying assets is the foundation of a cybersecurity risk management strategy and essential for prioritizing cyber defense. While the value of asset inventory usually goes unchallenged, too few organizations do it effectively, if at all. ICS network defenders need to understand which assets are on their networks and what information those assets provide.

There are multiple methods for discovering assets. The best approach will likely include multiple methods. The SANS ICS Security Blog post, "Know Thyself Better than the Adversary – ICS Asset Identification and Tracking," discusses four approaches to asset identification: physical inspection, passive scanning, active scanning, and configuration analysis.

Asset Inventory Database

An accurate and comprehensive asset inventory is much more than a list of devices. Data, processes, personnel and supporting infrastructure and dependencies to other systems should also be identified. An asset repository should include all components on the IT and OT networks and in the field, including third party and legacy equipment. The inventory record should be granular enough for appropriate tracking and reporting. Details should include but not be limited to asset owner, location, vendor, device type, model number, device name, hardware/firmware/software versions, patch levels, device configurations, active services, protocols, network addresses, asset value and criticality. Furthermore, an asset inventory is not a singular task, but an ongoing process. One approach to keeping the asset inventory current is to incorporate it into change management processes.

Unauthorized Assets

Performing an inventory will help reveal blind spots by identifying things that do not belong, such as a rogue wireless access point or other unapproved devices or connections. Inventories also illuminate processes and procedures that could enable the detection of unauthorized configuration changes or other anomalies within the environment.

Physical Inspection

An asset inventory would be incomplete without physical inspection. Network scanning methods reveal what is connected to the network at the time of the scan but may not readily account for disconnected devices that could be connected later, such as rogue or wireless devices. Additionally, a network diagram showing the relative physical locations and roles of the assets is essential for thoroughly documenting the system.

Vital Data

Not only is the asset inventory a foundation for cyber defense, it is also vital information for incident response (Fundamental 11). In the same way asset inventory and network diagram documentation are of paramount importance to the asset owner, they are also very attractive to an adversary. Hence, this information needs to be as rigorously protected as the ICS system itself (Fundamental 5).

Resource Links

- Know Thyself Better than the Adversary – ICS Asset Identification and Tracking (SANS ICS Security Blog)
- Understanding OT/ICS Asset Discovery: Passive Scanning vs. Selective Probing (Ralph Langner)
- The Time for IT Asset Management Is Now (IBM Security Intelligence)
- Energy Sector Asset Management (NIST/NCCoE)
- ICS Cybersecurity: Protecting the Industrial Endpoints That Matter Most (PAS Global)
- ICS Cybersecurity: You Cannot Secure What You Cannot See (PAS Global)

2. Assess Risks

Risk assessments are instrumental in identifying security gaps and vulnerabilities. They are vital to prioritizing the application of controls and countermeasures to protect the organization. Once asset inventory has been completed or updated, thorough and regular risk assessments must be conducted to identify and prioritize (or re-prioritize) risk to key assets. The importance of risk assessments cannot be overstated. Indeed, risk and resilience assessments are now required of drinking water systems every five years per the America's Water Infrastructure Act (AWIA) (S. 3021; Public Law 115-270, enacted October 23, 2018,) which amended Sec. 1433 of the Safe Drinking Water Act.

Risk is a function of vulnerability, threat and consequence but is often daunting to measure. The goal of a risk assessment is to identify and prioritize risk based on the likelihood that a threat or vulnerability could adversely impact an organization. There is no one-size-fits-all process for performing risk assessments. However, several free and voluntary programs and frameworks are available to assist organizations in determining their security posture, which includes assessing risk of its people, processes and technologies.

While not a risk assessment standard *per se*, the National Institute of Standards and Technology (NIST) Cybersecurity Framework is one of the foremost resources for informing risk assessments. It was originally released in 2014 in response to Executive Order 13636. Updated in 2018, the framework provides a prioritized, flexible and free approach to managing cybersecurity risks. It has been designed to help organizations better understand, manage and reduce cybersecurity risk and to foster relevant conversations across organizational stakeholders.

The American Water Works Association (AWWA) risk assessment standard, "J100-10: Risk and Resilience Management of Water and Wastewater Systems," provides guidance on conducting risk assessments. It documents a process for identifying vulnerabilities to man-made threats, natural hazards and dependencies, and provides methods to evaluate the options for improving weaknesses.

Specifically designed for water and wastewater utilities is the "AWWA Cybersecurity Guidance & Tool," which provide a water sector-specific approach to applying the NIST framework. The AWWA cybersecurity resources have been recognized by the Water Sector Coordinating Council, the U.S. Environmental Protection Agency (EPA), the Department of Homeland Security, NIST and multiple states as the baseline for assessing cybersecurity risk management. Through posing a series of use cases designed to best represent a utility's application of various technology, the AWWA cybersecurity tool generates a report with prioritized controls that, if implemented, can help the utility mitigate cyber risks. Updated versions of the guidance and tool are due out in the summer of 2019. The updates will broaden their scope to address cybersecurity provisions in AWIA and enhance the functionality of the output to support utility self-assessment of the implementation status of recommended controls.

Another helpful tool is the EPA Vulnerability Self-Assessment Tool (VSAT,) which is compliant with the J100-10 standard. VSAT is a web-based tool that steps a utility through producing an assessment. According to EPA, a utility can use the tool to identify the highest risks to mission-critical operations and find the most cost-effective measures to reduce those risks. EPA has also produced

An additional resource may be NIST's SP 800-30 "Guide for Conducting Risk Assessments." SP800-30 provides guidance for carrying out each step in the risk assessment process.

The Department of Homeland Security's National Cybersecurity and Communications Integration Center (DHS NCCIC) Critical Infrastructure Assessment Program offers many free products and services to help raise awareness, identify security gaps and provide recommendations to assist organizations in managing cyber risk. Several consulting firms also provide these services.

The outcome of any risk assessment will provide an organization with a current risk profile and inform prioritization of the initiatives that will improve the cybersecurity posture. In that context, fundamentals 3 through 15 are designed to provide general guidance to assist water and wastewater utilities when applying the necessary controls and countermeasures identified through the risk assessment process.

Resource Links

- America's Water Infrastructure Act (WaterISAC)
- Cybersecurity Framework (NIST)
- Cybersecurity Framework Reference Tool (NIST)
- Cybersecurity Guidance and Tool (AWWA)
- Cybersecurity Risk and Responsibility in the Water Sector (AWWA)
- J100-10 Risk and Resilience Management of Water and Wastewater Systems (AWWA)
- Vulnerability Self-Assessment Tool (US EPA)
- Guide for Conducting Risk Assessments – SP 800-30 (NIST)
- DHS NCCIC Cybersecurity Assessment Tools (WaterISAC)

3. Minimize Control System Exposure

It is particularly important to understand any communication channels that exist between the industrial control system (ICS) network and other internal networks. According to critical infrastructure site assessments performed in the water and wastewater sector by NCCIC for FY2017, the most commonly identified weakness is a lack of appropriate boundary protection controls.

While isolating a control system from the rest of the world would be ideal, it may not be possible. Connections are difficult to avoid given the practical demands for remote system access by vendors and staff and due to the need to export control system data for regulatory and business purposes.

Even if these connections could be avoided, there are always control system upgrades and patches that make some kind of interface with the outside world unavoidable. Minimizing control system exposure requires a combination of physical and logical network segmentation, devices and software that restrict traffic, protection of control system design and configuration documents, encrypted communications, restrictive procedures and physical security.

External (Untrusted) Pathways

The control systems of some organizations may not directly face the internet. However, a connection likely exists if those systems are connected to another part of the network, such as the enterprise IT network, that has a communication pathway to or from the internet. These connections can be identified through a comprehensive asset inventory (Fundamental 1) and evaluated with a thorough risk assessment (Fundamental 2).

As most compromises to ICS networks emanate from the IT/business network, it is vital to eliminate any unnecessary communication channels discovered between devices on the control system network and equipment on other networks. Any connections that remain need to be carefully evaluated, managed and strengthened to reduce network vulnerabilities.

Similarly, a utility may have equipment or components that use Bluetooth or other short-range communications protocol for configuration. Despite the limited communication range of such devices, these connections represent another entry point for an adversary. Organizations may be unaware of these short-range connections, but cyber threat actors can find such pathways to access and exploit industrial control systems.

Segmentation

Access to network segments can be restricted by physically isolating them entirely from one another, which is optimal for industrial control systems, or by implementing technologies such

as firewalls, demilitarized zones (DMZs), virtual local area networks (VLANs), unidirectional gateways and data diodes.

- A **firewall** is a software program or hardware device that filters inbound and outbound traffic between different parts of a network, or between a network and the internet.
- An **ICS-DMZ** is a network segment that sits between the control system network and any untrusted or other internal network to protect unwanted traffic from communicating directly with critical devices within the control system zones.
- **VLANs** are logical connections that partition different segments of a network, often by function.
- **Unidirectional gateways** and **data diodes** allow for one-way traffic from the control system network and prevent traffic from flowing back into the control system network.

Zone Restrictions

Network segmentation also entails classifying and categorizing IT and ICS/OT assets, data and personnel into specific groups or zones, and restricting access based on these groupings. By placing resources into different segments of a network, and restricting access to specific zones, a compromise of one device or system is less likely to translate into the exploitation of the entire system. When interconnected, cyber threat actors may be able to exploit any vulnerability within an organization's system – the weakest link in the chain – to gain entry and move laterally throughout a network to access sensitive equipment and data. Given the rise of the "industrial internet of things" (IIoT,) whereby many previously non-internet connected protocols are being replaced with protocols like EtherCAT and Modbus TCP/IP to access greater automation, the importance of segmenting and partitioning networks is greater than ever.

Restrict Traffic

When installed and configured properly, firewalls, ICS-DMZs, VLANs, unidirectional gateways and data diodes provide crucial functions in filtering or blocking unwanted traffic that could adversely impact availability, reliability and safety of the control system network. By reducing the number of pathways into and between networks and by properly implementing security protocols on the pathways that do exist, it is much more difficult for a threat actor to compromise the network and gain access to other systems.

Creating network boundaries and segments and classifying assets and data empowers an organization to enforce both detection and protection controls within its infrastructure. The capability to monitor, restrict and govern communication flows provides a practical ability to baseline network traffic, especially traffic traversing a network boundary, and identifies anomalous or suspicious communication flows. These boundaries provide a means to detect potential lateral movement, network foot-printing and enumeration, and device communications attempting to traverse from one zone to another. To ensure unwanted traffic is not traversing the

network, firewall and segmentation rules should be reviewed regularly to assess the status of unnecessary ports or services.

Encrypted Communications

Another way to limit control system exposure is to encrypt all communications. Encryption can protect control system maintenance traffic on an internal network, external remote access traffic destined to the control system, or device-to-device traffic over the public telecommunications network or private radio network.

Protocols like IPSec can be used to encrypt traffic over a public telecommunications network. Built-in encryption options or add-on serial traffic encryption devices can be used to protect data radio communications. Encryption makes it very difficult for malicious actors to fake or intercept control system traffic.

An alternative approach under certain circumstances is to configure IPSec for authentication only. This approach provides data integrity to prevent malicious manipulation but still allows asset owners to easily perform traffic inspection.

Restrictive Procedures

Only dedicated and properly secured devices should be permitted within the control system environment, and each one should be clearly marked as such. This applies to staff, contractors, consultants and vendors regarding use of laptops, memory flash drives, backup hard drives and any other device that could be infected with malware, including mobile and "internet of things" (IoT) devices. During periods of large-scale control system enhancements or upgrades, additional separation measures may be needed, such as requiring the integrator to use utility owned laptops and software, or possibly developing and testing the new system on a parallel network not connected to the active control system.

While external connections to the control network should always be disabled, that may not be practical. There are instances where a connection is necessary and exceptions must be made for updates, remote administration, vendor access or other reasons. In these instances, employing an ICS-DMZ is necessary to secure the communication pathways between the networks for those occasions when secure access is temporarily enabled.

Once access is no longer needed, connections must be disabled immediately. Never leave a connection to the control network enabled for an undetermined timeframe. Likewise, in lieu of enabling temporary network access, consider requiring the use of a dedicated and hardened, non-ICS connected PC for things like patch downloads. Downloads should be scanned for malicious content, and cryptographic hashes or digital signatures validated before applying to control system devices.

For more rigor on minimizing control system exposure, utilities are highly encouraged to incorporate the NCCIC's recommended practice, "Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies," into their cybersecurity strategies.

Resource Links

- Recommended Practice: Improving Control System Cybersecurity with Defense-in-Depth Strategies (DHS NCCIC)
- Secure Architecture Design (DHS NCCIC)
- Guide to Industrial Control Systems (ICS) Security – SP 800-82 (NIST)
- Building Cybersecurity Firewalls (Control Global)
- Data Diodes Protect Critical Water Infrastructure (Fend)
- Data Diode Cyber Security for Water & Wastewater Utilities (OWL Cyber Defense) (Sign up required)
- Keeping Industrial Facilities Safe - The Importance of Network Segregation (Applied Risk)
- Control Systems Communications Encryption Primer (DHS)

4. Enforce User Access Controls

Access control involves providing control system access only to those individuals who are authorized to have it. Restricting access to select individuals limits the number of people who can interact with key systems. When logging and auditing is enabled (Fundamental 10), this restriction also makes it much easier to detect suspicious and unauthorized access. Audit logs identify credentials associated with accidental, unapproved, or misconfiguration changes; the fewer credentials that have access, the more focused the investigation. Important components of access control include role-based controls, principle of least privilege, password management, secure remote access and off-boarding.

Role-Based Access Control

Role-based access control (RBAC) grants or denies access to network resources based on job functions or responsibilities. This control limits the ability of individual users – or attackers – to reach files or parts of the system they should not access. For example, SCADA system operators likely do not need access to the billing department or certain administrative files. Therefore, define permissions based on the level of access each job function needs to perform its duties. In addition, limiting employee permissions through RBAC can facilitate tracking network intrusions or suspicious activities during an audit.

Principle of Least Privilege

Similar to RBAC is the principle of least privilege. By applying the principle of least privilege to a user account, only the absolute minimum permissions necessary to perform a required task are assigned. In other words, administrative or other privileged accounts are reserved for special use and are not to be logged in perpetually. Most malware operates with permissions of the logged in user. By granting access and permissions based on roles and least privilege, malware has limited access to the resources it can compromise.

While the least-privilege approach is a defense against many types of malware, unpatched vulnerabilities can still be exploited to elevate privileges regardless of user access rights. Therefore, it is important to maintain an effective patch management regimen (Fundamental 7) to reduce vulnerabilities that could lead to privilege escalation attacks.

Password Hygiene

In June 2017, NIST updated its password guidance, reducing the user burden in an effort to improve password hygiene. While maintaining security, the new guidance seeks to reduce complexity requirements and encourage more user-friendly password policies. NIST updated the password guidelines to generally allow for longer passwords without the special character complexity restrictions. Essentially, this increased length and reduced complexity enables users to create longer but more memorable passwords or passphrases that are more difficult to

crack. NIST also advises that requiring users to change their passwords regularly makes memorizing them difficult and makes it more likely users will record their passwords in an unsafe manner.

Longer Passwords Are Better

Malicious actors use readily available software tools to try common passwords or millions of character combinations to attempt unauthorized logins. These are called "dictionary" and "brute force" attacks. In addition, users often make common character substitutions or additions that have become predictable and those variations have been added to the brute force/dictionary tools. To keep systems and information secure, enforce the use of longer passwords or passphrases that accommodate any ASCII printable character, and unique passwords for each account. Use password management software to keep track of multiple passwords.

No Default Passwords

When new devices or software are installed, it is imperative to change all default passwords, particularly for administrator accounts and control system devices. Many factory default passwords are widely known and discoverable through a simple Google or Shodan search. In addition, implement other password security features, such as an account lock-out that activates after too many incorrect password attempts.

Multifactor Authentication

Multifactor authentication decreases the risk that an adversary could log in with stolen credentials. Organizations should consider requiring multifactor authentication by verifying identity when each user attempts to log in. Common multifactor authentication methods include biometrics, smart cards, FIDO/CTAP (client to authenticator protocol) enabled hardware devices, or one-time passcodes sent to or generated by previously registered devices.

Secure Remote Access Solutions

The ability to remotely connect to a network adds a great deal of convenience for end users, engineers, systems administrators and support vendors, but it also provides an opportunity for threat actors to infiltrate your network. Methods of connecting securely should be implemented to minimize risk. Firewalls, demilitarized zones (Fundamental 3,) jump boxes, virtual private networks (VPNs), secure shell (SSH) and multifactor authentication are all methods that provide increased security when remote access is required. Additionally, remote access can further be restricted with access control lists that only allow access from specific IP addresses and/or ranges and geographic locations.

Jump Boxes

Jump boxes are intermediate servers that reside in the demilitarized zone (DMZ). When remote access is required, jump boxes are used for authentication and to provide connectivity to less secure remote servers in the control network. Jump boxes provide the ability for remote users to connect to an intermediary device without having to connect directly to control network servers, workstations or other less secure devices.

VPN

A VPN is an encrypted data channel to securely send and receive data via public IT infrastructure (such as the internet,) or to securely connect to the control network from other segments of the enterprise network. Through a VPN, users can remotely access internal resources like files, printers, databases, websites and management interfaces as if directly connected to the network. However, a VPN is only as secure as the devices connected to it; an authorized device infected with malware can propagate that malware onto the network, leading to additional infections and negating the security of the VPN.

SSH

SSH provides secure authentication and authorization to hosts when remote administration is required. SSH is used to safely and remotely connect to devices to perform management or file transfer activities. It should be disabled by default and access granted only to explicitly defined hosts and networks.

Off-Boarding

To protect company assets from unauthorized access, physical and cyber access should be disabled as soon as it is no longer required. Terminated and voluntarily separated employees, vendors, contractors and consultants should have access revoked as soon as possible. Likewise, employees transferring into new roles will likely need to have unnecessary access removed. A rigorous off-boarding procedure should be established with human resources and contract managers, as well as IT and OT staff. The off-boarding procedure should include an audit process to identify disabled and deleted accounts and to confirm appropriate access deprovisioning due to role transfers. The procedure should also incorporate a method to identify any shared accounts, like system administrator, development environment, application and vendor accounts.

Resource Links

- Configuring and Managing Remote Access for Industrial Control Systems (DHS NCCIC)
- Security of Interactive and Automated Access Management Using Secure Shell (SSH) (NIST)

- FIDO2 Project (FIDO Alliance)
- Role Based Access Control (NIST)
- Security and Privacy Controls for Federal Information Systems and Organizations – SP 800-53 (NIST)
- Implementing Least-Privilege Administrative Models (Microsoft)
- Choosing and Protecting Passwords (DHS NCCIC)
- Supplementing Passwords (DHS NCCIC)
- Digital Identity Guidelines – SP 800-63-3 (NIST)
- Password Guidance from NIST (NIST)

5. Safeguard from Unauthorized Physical Access

There is a common IT/OT adage, "If you can touch it, you own it." Therefore, it is imperative to limit physical access to IT and ICS environments, including communications equipment and assets at remote locations.

Physical access should be limited to only those who need it. The use of identification key cards, cameras, motion detectors, security personnel and intrusion alarms should be used to protect physical assets from unauthorized access. This includes excluding those attempting to piggyback along with authorized personnel.

Non-technical, physical barriers, like fences, barricades, gates, guards and locked doors should be used to establish a security defense around the perimeter of buildings containing IT and ICS equipment. Locked cabinets, cabinet intrusion alarms and conduits for network cables can be used to further protect IT and ICS equipment and systems from unauthorized physical access. The NCCIC's Recommended Practice, "Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies," covers many considerations regarding physical security measures to keep unauthorized individuals from gaining physical access.

Physical Penetration Testing

Utilities are encouraged to perform physical penetration tests at all facilities. Any network-based pen test engagements should also include attempts to breach defenses through on-site physical access, not just to test physical security, but to identify where a physical security breach could also lead to direct IT or OT system access.

Through social engineering techniques and by combing through social media, attackers can acquire knowledge of people and processes to gain unauthorized physical access to a facility. Physical infiltration could provide an attacker with access to privileged credentials written on sticky notes or in notebooks. This, in turn, could lead to attackers having direct network access, allowing them to plant remote hacking software or hardware tools to be leveraged later. At the very least, organizations should perform their own reconnaissance to learn what facility and employee information is publicly available. Unnecessary disclosures should be mitigated. Organizations can use the results of physical pen tests to increase staff awareness of physical and human vulnerabilities that they can avoid and mitigate.

Protection of Hardware

Gaining physical access to control rooms or other sensitive areas often implies gaining access to IT or ICS equipment, but this need not be the case if utilities apply additional physical security measures. For example, hard drives and portable media drives can be affixed with locks or removed and stored in secured containers when not in use. Organizations can also disable USB

ports, preventing someone from being able to upload or download data using a USB device. Buttons that control important functions such as power can be disabled, or feature physical protection devices that prevent unauthorized use. Authentication methods used for these functions such as keys and fobs can be stored in locked areas when not in use.

Furthermore, computers used for ICS functions should never be allowed to leave the ICS area, lest they be compromised when in less secure environments. Electronic devices that must be taken out of secured areas, such as laptops, portable engineering workstations, and handhelds should be tightly controlled and returned to secured areas when not in use.

Malicious actors are not the only threat to IT and ICS hardware; natural disasters can threaten this equipment as well. Therefore, organizations should implement measures that protect hardware from events like earthquakes, hurricanes and floods, which can damage equipment directly or have indirect impacts through the loss of power.

Protecting Design and Configuration Documents

If a threat actor cannot gain direct access to a control system, his or her next best option is to procure design and configuration documents. This information facilitates, and perhaps, even guarantees, a successful campaign by a threat actor. Ways to protect these digital and paper documents include encrypting digital copies, keeping physical paper copies in a locked office and cabinet, limiting control room tours and preventing visitor photography.

Likewise, it is important to limit the availability of sensitive documents during open procurements. Document access can be restricted through non-disclosure agreements, background checks, two-step procurement process with limited information provided during the qualification stage, secure file sharing with encryption, and document review only under supervision while onsite at the utility.

The importance of protecting control system design and configuration documentation was recently underscored by the North American Electric Reliability Corporation (NERC) in 2016. NERC fined one of its electric utility members $2.7 million for not properly protecting its critical cyber asset documentation, thereby unintentionally enabling a contractor to expose the documents on the internet.

Resource Links

- Recommended Practice: Improving Control System Cybersecurity with Defense-in-Depth Strategies (DHS NCCIC)
- Understanding the Importance of Physical Security for Industrial Control Systems (Applied Risk)
- NERC Full Notice of Penalty regarding Unidentified Registered Entity (NERC)
- The Social Engineering Framework (Social-Engineer, LLC)

6. Install Independent Cyber-Physical Safety Systems

Adversaries may compromise an IT or OT control system to seek monetary gain, perform reconnaissance, modify operations, weaken customer trust, injure people or physically destroy equipment or infrastructure. Malicious cyber actors targeting the water sector may seek long-term physical service disruption by breaking pipes or damaging large rotating equipment that have long replacement times. These types of cyber-attacks resulting in physical impact represent a complex, or blended, threat. To protect critical assets from blended threats, utilities should consider non-digital engineering solutions such as independent cyber-physical safety systems.

If we can protect our critical assets from physical damage, service disruption from a cyber-attack may be limited to the time it takes to transition to manual operation. Blended attacks with long-lasting impacts can be mitigated by physically preventing access to process equipment and by installing independent cyber-physical safety systems. These systems should prevent conditions such as excessive levels of pressure, chemical additions, vibrations or temperature change from occurring due to malicious acts against a compromised control system.

In 2007, Idaho National Labs dramatically demonstrated an example of a cyber-physical vulnerability in their experimental AURORA attack by remotely damaging a large diesel generator. During the demonstration, the generator's circuit breaker was rapidly opened and closed to force it out of phase with line power, which in turn created destructive electrical torque that physically damaged the unit.

Few utilities have cybersecurity experts readily available, but every utility already has staff and consultants who understand the intricacies of their water or wastewater processes and infrastructure. Existing staff can collaborate to identify ways that physical damage or hazardous situations can be created either intentionally or accidentally.

For example, a contingent of experienced staff should imagine worst case scenarios, assuming an attacker has full knowledge and total control of the OT system. What could the attacker do to cause injury or lasting system damage?

While we carefully protect against adverse conditions, if the protection comes from logic built into the control system, the system can still be compromised. It is critical to design and implement independent protections.

Example Solutions and Potential Precautions

In the same way that a large generator can be protected from an AURORA style attack with a properly designed protection relay, and a boiler can be protected from a low-water-explosion

with an independent low-water trip switch, vital components of water systems can also be protected.

For example, attempts to break pipes by valve water hammer or harmonics can be mitigated with appropriately slow mechanical gearing of valve actuators. Attempts to break pipes by turning on too many pumps within a pressure zone can be handled by independent pressure switches wired to pump controllers, or by increasing tank overflow capacity. Dangerous overdosing of treatment chemicals can be mitigated by careful pump sizing. Attempts to damage large rotating equipment through variable frequency drive manipulation can be countered with independent vibration monitoring interlocks. Attempts to run wastewater pumps dry for extended periods by falsely presenting high wet-well levels to the control system might be managed by creating a combined high RPM and low electrical current triggered interlock.

The independent and isolated aspects of a cyber-physical safety system are essential to its success. In 2017, the TRITON/TRISIS attack against a Saudi Arabian petrochemical plant demonstrated what could happen when a safety system is connected to a control system. In this case, the rigorous Safety Instrumented System required for hazardous chemical facilities was compromised, presenting the potential for serious damage and injury if the control system had been subsequently attacked.

Finally, it is very important not to reduce the overall reliability of water and wastewater service because of the design, implementation or maintenance of a cyber-physical safety system. Achieve simplicity and lower risk by using mechanical safety systems, such as a rupture disk. Use independent process monitoring alarms (Fundamental 5) in an initial, conservative approach. In some less time-sensitive cases, such as attempts to damage heat-sensitive electronic equipment by compromising an HVAC and building control system, use mechanical safety systems to reduce the likelihood of breach.

Resource Links

- Subject Matter Expert Workshop to Identify Cybersecurity Research Gaps and Needs of the Nation's Water and Wastewater Systems Sector (US EPA)
- The End of Cybersecurity (Harvard Business Review)
- Engineering Out the Cyber-Risk to Protect What Matters Most (Idaho National Laboratory at RSA Conference 2019) (sign-up required)
- Cyber-Informed Engineering (Idaho National Laboratory)
- Improving Safety in Process Control (Control Engineering)
- Cyber-Physical Attack Recovery Procedure (Luis Ayola, 2016)
- Mitigating the Aurora Vulnerability with Existing Technology (Georgia Tech Protective Relaying Conference)
- What You Need to Know (and Don't) About the AURORA Vulnerability (Power Magazine)

- Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure (FireEye)
- Triton/Trisis Attack was More Widespread Than Publicly Known (Dark Reading)

7. Embrace Vulnerability Management

Vulnerability management is at the core of every cybersecurity program. Like asset inventory (Fundamental 1) and risk assessments (Fundamental 2), it is a continuous process and completely dependent on and intertwined with those programs. Vulnerabilities are present everywhere – hardware, software, firmware, configurations, supply chains and staff practices. Therefore, vulnerability management is an absolute necessity in every organization. While tasks like patching and antivirus are important in addressing some vulnerabilities, effectively managing vulnerabilities requires a holistic program.

Identify Vulnerabilities Before the Bad Guys Do

With the number of IT devices and internet-accessible ICS devices increasing each year, vulnerabilities present an open window for a cyber-attack. Public resources like Shodan, Censys, and even Google enable the discovery of vulnerable devices by anyone with an internet connection. Combining data garnered from these discovery tools with vulnerability exploitation kit frameworks like Metasploit, novice threat actors are able to launch attacks with very little knowledge or understanding about the ICS systems they are targeting. Performing authorized scans and assessments, including penetration tests, will help identify vulnerabilities within your own environment before the bad guys do.

In its "Year in Review 2018 Industrial Control Vulnerabilities," ICS cyber forensics firm Dragos reports 57% and 55% of ICS-related vulnerabilities could cause a loss of view and loss of control, respectively, with 60% potentially causing both. This would likely result in severe operational impact if exploited. Dragos further suggests that while challenging to patch, the sheer percentage of vulnerabilities present in field and Purdue Level 1 and 2 devices indicates a decent likelihood of attack success should an attacker find its way onto the ICS network.

Information on vulnerabilities is provided from various sources including vendors, cybersecurity firms, ISACs and federal agencies. To aid utilities in maintaining awareness of vulnerability disclosures, **WaterISAC regularly disseminates information on vulnerabilities and patches received from partners at the U.S. Department of Homeland Security's NCCIC, other ISACs and cybersecurity firms, among others.** These curated advisories and bulletins are invaluable, but utilities need to have an internal program to further track, research and effectively address disclosed vulnerabilities in a way that is most appropriate and relevant to each environment.

Remediate/Mitigate

Once vulnerabilities have been identified and prioritized, they must be remediated, mitigated or accepted. Device vulnerabilities are frequently remediated through patching and updating software and firmware. However, even after patches and updates have been released, many systems remain vulnerable because organizations are either unaware or choose to not implement fixes due to lack of understanding or insufficient resources.

Furthermore, some products have design "features" that are inherently insecure and will never have a patch. In instances where patches are not or cannot be applied, vulnerabilities should be mitigated through compensating security control methods such as "hardening" to remove unnecessary services and applications, replacing devices when they are no longer supported by the vendor, enforcing policies and procedures (Fundamental 9), and providing cybersecurity awareness and technical training (Fundamental 8). Impacts can be further reduced by installing independent cyber-physical safety systems (Fundamental 6), interrupting threat actors early in the attack cycle through successful threat detection (Fundamental 10), and applying lessons learned post-incident response (Fundamental 11).

Resource Links

- Year in Review 2018 Industrial Control Vulnerabilities (Dragos) (sign up required)
- Exposed and Vulnerable Critical Infrastructure: Water and Energy Industries (WaterISAC)
- Recommended Practice for Patch Management of Control Systems (DHS NCCIC)
- Recommended Practice: Updating Antivirus in an Industrial Control System (DHS NCCIC)
- What Does "Insecure By Design" Actually Mean for OT/ICS Security? (Langner)
- The Five Things You Need to Know About OT/ICS Vulnerability and Patch Management (Langner)
- Index of Advisories by Vendor (DHS NCCIC)
- National Vulnerability Database (NVD) (NIST)
- Common Vulnerabilities and Exposures (CVE) (MITRE)
- Enabling Continuous Vulnerability Management for Industrial Control Systems (ARC Advisory Group)

8. Create a Cybersecurity Culture

Cybersecurity is a shared responsibility among all staff. Every employee, executive and board member is accountable for the overall cybersecurity posture of an organization. When employees are not involved in cybersecurity, not only can vulnerabilities and threats go unnoticed, but employees often become unintentional insider threats (Fundamental 12) or conduits through which attacks are executed, as cyber attackers continue to shift from hacking computers to hacking people. The SANS report, "Creating Environments for Successful Awareness Programs: Security Awareness for Executives," states that in many ways, advancements in security technologies have made humans an easier target. Creating a cybersecurity culture relies on leadership support and training and awareness programs.

Executive and Board Engagement – Leadership is Crucial for Culture Change

Effective cybersecurity starts at the top. Unfortunately, research reveals that organizational leaders still lack sufficient awareness of cybersecurity threats and needs. Organizations are increasingly elevating cybersecurity to the executive level by adding the role of Chief Information Security Officer (CISO) or Chief Security Officer (CSO). However, many organizations remain unprepared to manage cyber risk due to a lack of understanding, commitment, participation or empowerment from the C-suite and/or board of directors.

PwC's 2018 report, "Strengthening Digital Society Against Cyber Shocks," states that C-suites must lead the charge and boards must be engaged. A top-down strategy is essential to managing cyber risk across an organization. The report further states that most corporate boards are not proactively shaping their companies' security strategies or investment plans. This lack of support results in overall ineffective impact and inadequate behavioral and organizational culture changes.

There are many resources to facilitate leadership engagement. The NCCIC fact sheet, "ICS Cybersecurity for the C-Level," provides examples of six cybersecurity risk oversight questions every C-level executive should be asking about their environment. To further assist executives responsible for ICS environments, the document includes services and practical action steps specific to critical infrastructure. In addition, the SANS report, "Creating Environments for Successful Awareness Programs: Security Awareness for Executives," proposes multiple action items on ways leadership can voice support for cybersecurity programs.

Cybersecurity Awareness Training

The National Cyber Security Alliance (NCSA) promotes creating a culture of cybersecurity from the break room to the boardroom. Creating a cybersecurity culture through awareness training is a key organizational risk strategy component to manage human cyber risk by affecting behavioral change. To create and maintain a culture of cybersecurity, all personnel should receive regular, ongoing cybersecurity awareness training. In addition, role-specific training

should be provided for commonly targeted staff like executives, executive assistants, engineers, SCADA staff, IT administrators, operators, human resources and finance personnel. A SANS survey, "Securing Industrial Control Systems 2017," revealed an encouraging 59% of organizations implemented security awareness training for all personnel with access to control systems and control system networks.

While cybersecurity is an expansive subject, there are certain principal topics that should be regularly emphasized for general awareness and to promote positive cyber hygiene. One common theme that warrants frequent inclusion in training materials is social engineering, such as phishing, as it continues to be a popular tactic cyber criminals use to prey upon unsuspecting employees. Training should regularly incorporate the importance of safe internet browsing practices, as well as best practices for secure email handling.

Advanced Training for Technical Staff

In addition to role-specific training, utility OT, IT and legal staff should all be introduced and encouraged to delve into advanced cyber security training. Many free training opportunities are available online and in person.

If the utility is a state or local government organization, there are a variety of classes available from the Federal Virtual Training Environment (FedVTE). There are a number of free classes available through DHS at Idaho National Laboratory (INL) and classes hosted virtually. Hands-on red team/blue team exercises are available as part of the Industrial Control Systems Cybersecurity (301) training course. Access other training opportunities through the National Initiative for Cybersecurity Careers and Studies (NICCS) Education and Training Catalog. Excellent ICS cybersecurity conferences are held semi-annually by the Industrial Control System Joint Working Group (ICSJWG). WaterISAC and other organizations such as SANS, the Electricity ISAC and the Multi-State ISAC hold regular, insightful webinars.

Participation in national and regional cyber drills is another valuable training experience. Since defense is informed by offense, to help defenders think like adversaries, attending grey- or black-hat conferences is another valuable approach. Finally, holding monthly internal, cross-sectional meetings with staff involved in all aspects of cybersecurity, is a valuable practice to reinforce the importance of remaining vigilant. This team should discuss threats and vulnerabilities in the news, as well as organizational concerns, successes and priorities.

Benchmarking Your Cybersecurity Awareness Program

Statistics show that many organizations report having some sort of cybersecurity awareness program throughout various levels of maturity, with most being near entry-level. "The 2018 SANS Security Awareness Report" discusses the Security Awareness Maturity Model and examines maturity levels by industry, including utilities. The benchmarks can be used to compare your program to peers and determine where you want your program to be. For

organizations just beginning to embrace cybersecurity awareness, the report provides impactful action items for new programs to take on. Your program's success will result in widespread cultural acceptance of positive cyber hygiene behaviors and an increased cybersecurity readiness that will far exceed the investment.

Resource Links

- Creating Environments for Successful Awareness Programs: Security Awareness for Executives (SANS Institute) (sign up required)
- Strengthening Digital Society Against Cyber Shocks (PwC)
- Cybersecurity Questions for CEOs (DHS NCCIC)
- ICS Cybersecurity for the C-Level (DHS NCCIC)
- 2018 SANS Security Awareness Report: Building Successful Security Awareness Programs (SANS Institute)
- Avoiding Social Engineering and Phishing Attacks (DHS NCCIC)
- Securing Your Web Browser (DHS NCCIC)
- Best Practices for Dealing with Phishing and Ransomware (Osterman Research)
- Five Tips to Help Execute an Employee Training Program (Help Net Security)
- OUCH! Newsletter (SANS Institute)
- STOP. THINK. CONNECT.™ (National Cyber Security Alliance)
- Federal Virtual Training Environment (FedVTE) Course Catalog (DHS)
- ICS Virtual Learning Portal (DHS NCCIC)
- ICS-CERT Training Courses (DHS)
- NICCS Education and Training Catalog (NICCS)

9. Develop and Enforce Cybersecurity Policies and Procedures (Governance)

Developing policies and procedures can be one of the easiest and hardest fundamentals to implement. Regardless of difficulty, it is crucial to develop and enforce clear and actionable cybersecurity policies and procedures for all IT and OT systems. Policies and procedures should plainly define an organization's cybersecurity requirements.

For example, the fundamentals in this document each require policies and procedures. Once formalized, policies and procedures are operationalized through dissemination, communication, education and enforcement. Distributing and communicating cybersecurity policies throughout the organization is vital. All staff must be made aware of their responsibility to uphold policy, as well as the consequences of any violation.

The general term for this prescriptive staff guidance is governance. Governance is important and serious. In some instances a violation of a policy or procedure may even activate a utility's cybersecurity incident response plan (Fundamental 11).

Rinse, Repeat, and Audit

Governance is a continuous endeavor. Organizational environments and cybersecurity requirements are dynamic. Like all of the guidance presented, policies and procedures are not one-and-done. They need to be reviewed regularly, updated when necessary and subsequently communicated as changes are made. Furthermore, policies and procedures must be regularly audited for accuracy, understanding, and compliance among staff.

Policy Examples

The guidance in this document is a good place to begin developing cybersecurity policies and procedures for your utility. Other policy examples would be acceptable use of equipment and computing systems (including email,) vendor/supply chain risk management, mobile device management including internet of things, insider threats and disaster recovery.

The SANS Institute provides a set of templates covering important security requirements that can be customized to jump-start your policy development and implementation. In addition, DHS published the "State Cybersecurity Governance Case Studies Cross Site Report," which demonstrates how cybersecurity has been governed as an enterprise-wide, strategic issue across state government and other public and private sector stakeholders.

Resource Links

- Information Security Policy Templates (SANS Institute)

- 9 Policies and Procedures You Need to Know About if You're Starting a New Security Program (CSO Online)
- Cybersecurity Governance Publications (DHS)

10. Implement Threat Detection and Monitoring

While many of these cybersecurity fundamentals are developed with prevention in mind, in this "assume breach" world, we must be able to detect nefarious activity.

Logging and auditing internal systems, using passive or active cybersecurity monitoring systems, and employing independent process monitoring are valuable detection methods. Furthermore, by establishing a security operations center (SOC) and by integrating an ICS focus into the SOC, organizations are better able to leverage those tools and methods to proactively defend their ICS networks. Following threat and analysis reports provided by WaterISAC, DHS, FBI and others is an effective way to maintain awareness of critical infrastructure threat trends. These reports include threat actors' tactics, techniques and procedures (TTPs) and other indicators of compromise to help detect potential intrusion activity within your environment.

One significant advantage in monitoring a control system is the relatively stable hardware design and traffic patterns. This stability creates a baseline that monitoring systems can use to watch for changes in equipment configurations or activity.

Logging and Auditing

Detailed logs are essential for monitoring system, application and network activity. Properly configured logs enable organizations to conduct thorough root-cause analyses to find the source of issues or suspicious activity. Once enabled, logs are often collected and aggregated into a security information and event management (SIEM) system for real-time analysis and correlation. SIEMs ingest event logs from systems like firewalls, VPNs, intrusion detection systems and intrusion prevention systems, anti-virus software, proxy servers, end-user devices, servers and applications. Continuous auditing of logs allows organizations to discover unauthorized activity.

According to NCCIC/ICS-CERT site assessment findings, while most organizations enable logging, many fail to aggregate relevant logs to a centralized log management system or SIEM for correlation and analysis. Even after configuring, many organizations neglect to regularly review logs for unusual and suspicious activity.

Passive, Active, or Hybrid Monitoring

Many commercial ICS-oriented cybersecurity monitoring systems are now available. These can provide control system inventories, detect unauthorized connections, including mobile devices, and spot potentially malicious activity. Non-commercial software is also available to provide similar monitoring by using low cost network taps.

ICS monitoring solutions are either passive, active or hybrid. Passive monitoring is essentially eavesdropping on the network and hoping to get useful information at some point; it is less risky

but could be time consuming and incomplete. Active monitoring involves scanning or polling the network with requests for specific information; it carries more risk but also provides more timely and complete data. Hybrid monitoring ostensibly offers the best of both worlds, providing some benefits of active monitoring without some of the potential risks historically experienced in ICS environments by active solutions.

There is likely no single monitoring solution that is right for every ICS environment, but perhaps a combination of solutions that evolve over time. As suggested by Belden's Zane Blomgren, a complete monitoring solution in a complex industrial automation environment does not need to be 100% passive or 100% active, or even 100% hybrid. The best monitoring solution often consists of a combination of tools that will provide the most comprehensive visibility and network reliability.

Regardless of preferred monitoring solution, without the ability to detect threats within your environment, adversaries will go unnoticed. Once a solution is implemented, monitoring can be performed in-house by the SOC, or by a managed security service provider (MSSP).

Independent Monitoring of Critical Instrument Values

If an adversary gains access to a control system, they can hide malicious activity by registering false readings on the control system displays. Utilities can counter this by identifying the most important process readings, such as a particular tank or wet well level, the pressure at an important distribution system location, or a specific water treatment chemical concentration. These critical measurement points can be monitored independently from the control system by connecting their milliamp signals to independent data loggers with real-time reporting and alerting. If the instrument is connected to a communications protocol that could be compromised, a separate instrument should be installed and monitored by the data logger.

In the event of a normal water or wastewater system problem, both the process control system alarms and the independent data logger alarms should trigger. If only the data logger alarms trigger, that could indicate a problem with the instrument, control system or an active cybersecurity incident. Operations staff can check the alarm comparison manually and investigate discrepancies. Another approach is to establish automated divergence alarms outside of the control system for when the two instrument values separate by more than an acceptable amount or percentage.

Security Operations Center

Building an ICS-centric SOC, or incorporating ICS-specific functions into an existing SOC, must combine the people, processes and technology necessary to detect and prevent an ICS cyber incident. One of the primary capabilities of a SOC is to gather, correlate and analyze network, host and application security events, typically through SIEMs and other event detection

technologies. SIEMs provide an interface to aid SOC analysts in detecting and alerting on anomalous activity and indicators of compromise.

In April 2018, Bitdefender published a survey report, "CISOs' Toughest Dilemma: Prevention is Faulty, yet Investigation is a Burden," that evaluated the biggest challenges to organizational cybersecurity in the absence of a SOC. Ultimately, an organization without a SOC lacks the ability to quickly investigate or respond to suspicious activity and potential threats. They also have less visibility into the network environment, thus impeding the ability to detect attackers already lurking within.

Resource Links

- Targeted Cyber Intrusion Detection and Mitigation Strategies (DHS NCCIC)
- Privilege Escalation (MITRE Adversarial Tactics, Techniques & Common Knowledge)
- The Four Types of Threat Detection (Dragos)
- Network Monitoring: Passive, Active or Both (Belden)
- Insights into Building an ICS Security Operations Center (Dragos)
- What is SIEM software? How it Works and How to Choose the Right Tool (CSO Online)
- What is the Difference Between a SOC and a CSIRT? (Rapid7)
- How to Structure Your CSIRT or SOC Team (InfoSec Institute)
- ICS Cybersecurity Requires Active and Passive Defense (ARC Advisory Group)
- CISOs' Toughest Dilemma: Prevention is Faulty, yet Investigation is a Burden (Bitdefender)

11. Plan for Incidents, Emergencies and Disasters

Developing plans for how the utility will respond to incidents, emergencies and disasters is critical for recovering from such events quickly. IT and OT should be concerned primarily with cyber incident response plans and disaster recovery plans. These are just two elements of, or adjuncts to, overall business continuity or continuity-of-operations plans.

These plans should not be developed by a single department, but rather in collaboration with all departments. Including external stakeholders such as emergency response and law enforcement authorities in the development of the plans can also be valuable. This holistic inclusion will ensure a cooperative and unified response that leverages all of an organization's resources to the greatest extent possible.

Cyber Incident Response Plan

Despite established safeguards, many organizations still experience cybersecurity compromises. Indeed, experts note experiencing a compromise is not a matter of if, but when. However, organizations that fare best will be those that are able to quickly detect the intrusion (Fundamental 10) and have a defined plan in place to respond. An effective cyber incident response (IR) plan will limit damage, increase confidence of partners and customers and reduce recovery time and costs. Nevertheless, research reveals incident response plans are underutilized.

The ability to detect any cyber intrusion requires properly configured and maintained threat detection and logging (Fundamental 10). Without threat detection and logs from network hosts and applications, it is difficult to identify how an incident occurred, and nearly impossible to determine its scope. Furthermore, the cybersecurity response plan needs to be in place before an incident occurs and should be incorporated into enterprise business continuity plans.

Cyber Incident Response Team

For enhanced response capability in the event of a cybersecurity incident, organizations should consider forming a cyber incident response team to develop and manage the incident response process. The SOC (Fundamental 10) is responsible for day-to-day investigations, but a separate team should be established to respond to critical cybersecurity incidents. The cyber incident response team should develop the incident response governance model (Fundamental 9), including defining the types and severity of incidents that will require a comprehensive response.

The cyber incident response team should be comprised of organizational stakeholders, including other departments and external entities. In addition to IT and OT security staff and operators, team composition should include other staff such as executives, communications and public relations teams, human resources, legal, product and engineering personnel.

Cybersecurity Insurance

Recovering from a cybersecurity incident can be an expensive proposition. Average estimates for the cost of cyberattacks run from tens of thousands of dollars for small organizations to millions of dollars for large organizations. Expenses can include emergency support of vendors that specialize in incident forensics and recovery, replacement of corrupted software, computers and other hardware, complimentary credit monitoring for customers whose data was stolen, customer notification, lost productivity of employees who cannot work until the system has been restored, legal fees and liabilities and, in the case of some breaches, even public relations outreach.

Cybersecurity insurance is a tool in the resilience toolkit. Not only can insurers reimburse or pay for some or all expenses listed above, some policies provide expert emergency support in the form of knowledge and vendors and contractors specializing in forensics and recovery. However, cybersecurity insurance is still a relatively new market and policy exclusions vary from vendor to vendor, so researching insurers and comparing products is important.

For instance, some policies may not pay claims for pre-existing breaches, acts of war, or if the cause of the breach was an employee who fell victim to a phishing email or other social engineering tactic. Insurers may insist on minimum required security controls, risk assessment or cyber risk profile before granting a policy.

Disaster Response Plans

Under America's Water Infrastructure Act, drinking water systems must develop emergency response plans (ERPs) and update them every five years. The plans must address both cyber systems and physical systems. The plans required under the act go beyond emergency response. The law's provisions require utilities to document how they will mitigate threats and how they will enhance their mitigation and resilience, too.

While ERPs are not required for wastewater utilities under the law, these utilities may find it useful to prepare them. Regardless of the law, these plans can provide guidance during times of heightened confusion or stress. For this reason, plans help reduce the severity of impacts and facilitate a faster recovery for the system and the affected organization's overall operations.

IT and OT professionals may be more familiar with the concept of the disaster response plan (DRP), which can be folded into a utility's ERP. Both of these documents are traditionally part of an organization's business continuity plan or continuity of operations plan, which is described in the Water Research Foundation's "Business Continuity Planning for Water Utilities."

During the preparation of the emergency response plan, input should be obtained from various stakeholders, which can include personnel from IT, OT and physical security departments of the organization and others. All stakeholders should regularly train on and exercise the plan.

DRPs can include:

- A list of major goals of the disaster plan.
- Names and contact information of IT and OT personnel, vendors and contract support.
- Roles and responsibilities.
- Profiles of software and hardware used by the utility, including a discussion of which utility functions rely on each software and hardware item.
- Service level agreements for outsourced services during a disaster.
- Recovery time objectives.
- Maximum tolerable downtime.
- Backup procedures.
- Plans for mobilizing to temporary work locations.
- Plans for backing up to a temporary site.
- Plans for restoring the home site.
- Plans for testing and exercising the DRP.

Power Resilience

Utilities require power to operate their IT and ICS equipment, and they can protect their systems against the impacts of power outages by having on-site generation available in emergencies. Generators can be either utility-owned or supplied during an incident through preexisting contracts. NIST encourages utilities to have an uninterruptible on-site power supply that can span the time between when power is lost, and emergency power generation is activated. Utilities should also have plans in place to ensure that generators will have adequate fuel throughout an emergency situation. Water utilities can also coordinate with their local power utility to ensure that critical facilities are a high priority during power restoration efforts. Additional information about power outage resilience is available on WaterISAC's "Power Outage and Black Sky Resilience resources" web page.

Practice Makes Proficient

As is true for all response and recovery plans, IRs and DRPs are not complete once they have been developed; the plans need to be operationalized as well. The plans must be routinely reviewed and updated to ensure they remain relevant and usable when they are actually needed. Organizations should practice their plans through regular operational and tabletop exercises. To test readiness, considering incorporating a red team/blue team approach to the exercises.

Manual Operations

Manual control of water and wastewater systems should also be practiced as part of IR procedures to help understand limitations and inform design enhancements that can make future manual control more efficient.

IR plans should include measures for reacting to destructive malware in an ICS environment. In such situations, organizations should be prepared to restore from off-line backups and to "island" their ICS environments by disconnecting from non-ICS networks. They should also be prepared to revert to manual operations if network conditions impact visibility from the SCADA system, or if malware potentially renders control devices inoperable or untrustworthy.

Practice ensures that all stakeholders understand the procedures that would be implemented in the event of a significant cyber disruption or breach, enabling a more effective and efficient response.

Resource Links

- Incident Action Checklist – Cybersecurity (EPA)
- 6 Steps for Building a Robust Incident Response Plan (CSO Online)
- Creating an Incident Response Checklist to Prepare for a Data Breach (IBM)
- Ten Steps to Planning an Effective Cyber-Incident Response (Harvard Business Review)
- Best Practices for Continuity of Operations (Handling Destructive Malware) (DHS NCCIC)
- How Incident Response Fails in ICS Networks (Dark Reading)
- Develop and Conduct a Water Resilience Tabletop Exercise with Water Utilities (EPA)
- 7 Items You Must Add to Any Incident Response Plan (Symantec)
- Data Breach Insurance for NRWA members (NRWA/Beazley)
- A User's Guide to Data Breach Insurance Coverage (Risk Management Magazine)
- Transferring Cybersecurity Risk: Considerations When Obtaining Cyber Insurance (The National Law Review)
- Emergency Planning for Water & Wastewater Utilities - M19 (AWWA)
- Business Continuity Planning for Water Utilities (WRF)
- 8 Ingredients of an Effective Disaster Recovery Plan (CIO Magazine)
- Power Outage and Black Sky Resilience Resources (WaterISAC)

12. Tackle Insider Threats

Strong protective cybersecurity controls and system architecture can quickly be defeated by an adversary with physical or privileged access. It is common to believe our greatest threat is external and remote; however, an insider, whether an employee, visitor, vendor, contractor or consultant can cause as much or more damage. According to the Ponemon Institute's report, "2018 Cost of Insider Threats: Global," the average cost of insider-caused incidents was $8.76 million in 2017.

The more awareness employees have regarding cyber threats, the less likely they are to cause harm to critical assets or systems. In the "2017 U.S. State of Cybercrime" report, the U.S. Secret Service and the CERT division at the Software Engineering Institute at Carnegie Mellon University found nearly 30% of all respondents reported that incidents caused by insider attacks were more costly or damaging than outsider attacks. Likewise, nearly half (44%) of respondents indicated they could not identify the individual behind the incident, a 13% increase from the previous year.

What Makes an Insider a Threat?

An insider threat is a people problem, not a technology problem; without people, there would be no problem. The bottom line is that every person represents a potential insider threat. However, not all insider threats are malicious.

Many insider threats occur due to simple negligence, lacking intent or motive. A tired or distracted employee can make an honest mistake, or an employee who is unaware of a particular risk may not perceive how their actions could perpetuate a threat.

Incidents caused by unintentional actions commonly involve accidental disclosure of sensitive information, often precipitated by phishing. Individuals lacking intent or motive are generally referred to as "unintentional" or "inadvertent" insiders.

On the other hand, individuals with motive and intent to cause damage are considered "malicious" or "intentional" insiders. Malicious insiders typically experience some sort of psychological trigger that motivates them to act with malice, either caused by personal stressors or coercion. Malicious insiders typically commit criminal acts like fraud, theft, espionage or sabotage.

Start Somewhere

Not every organization has the resources to develop a formal insider threat program. While creating a culture of cybersecurity (Fundamental 8) among all levels of your organization will help deter or prevent many insider threats, it is not enough. Every organization needs to

implement some controls beyond security awareness efforts to prevent, detect, and respond to all types of insider threats.

Consider establishing a committee of relevant stakeholders to begin evaluating viable methods. The committee should have representation from key departments across the organization such as human resources, legal, information technology, cybersecurity, physical security and communications. The CERT Insider Threat Center's "Common Sense Guide to Mitigating Insider Threats, Fifth Edition" includes an appendix with quick wins and high-impact solutions to help you get started.

Resource Links

- Common Sense Guide to Mitigating Insider Threats, Fifth Edition (CERT Insider Threat Center)
- These 5 Types of Insider Threats Could Lead to Costly Data Breaches (IBM Security Intelligence)
- 2018 Cost of Insider Threats: Global (Ponemon Institute)
- 2017 U.S. State of Cybercrime (CERT Insider Threat Center & U.S. Secret Service)

13. Secure the Supply Chain

As outlined in Fundamental 12, vendors, contractors, consultants and integrators represent possible insider threats to an organization. They also constitute vital parts of the supply chain. A common supply chain compromise involves attackers infiltrating smaller vendors or suppliers to gain a foothold into larger entities. Therefore, these relationships must be assessed and better managed for the risks they pose to the overall risk profile of an organization.

"You are only as secure as your weakest link" is a phrase all too appropriate to describe the risk from supply chains. Attackers are keenly aware that smaller businesses are usually not as cyber secure as the larger companies with whom they contract. The Target breach in 2013 is still one of the most highly referenced examples of how the compromise of a small vendor was used to infiltrate a major corporation. This breach was carried out due to a successful spear phishing attack against a small, less cyber-prepared vendor.

In addition to spear phishing, adversaries have other techniques at their disposal, such as network pivoting and weaponizing software installs. The NCCIC's recommended practice, "Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies," lists typical supply chain compromises that occur in the IT and ICS environments. These supply chain compromises often include malware and vulnerabilities found in hardware and software components.

As cybersecurity firm Dragos recounts, one of the most notable cascading supply chain attacks that affected industrial organizations was NotPetya malware, also known as Nyetya. A compromise disguised as ransomware and designed to affect one software application, the malware subsequently scanned IP address ranges and spread to non-targeted third-parties and business partners, ultimately crippling major global corporations including FedEx and Maersk.

In its report, "Exposed and Vulnerable Critical Infrastructure: Water and Energy Industries," TrendMicro provides advice for managing supply chain threats. The recommendations include performing risk assessments of all suppliers and vendors in your supply chain, performing security and vulnerability testing on third-party software, and periodic background checks on all temporary and contracted personnel.

Furthermore, employee awareness (Fundamental 8) cannot be overstated in helping curb threats from third parties. Attackers usurp the foundation of trust that is built between a company and its vendors. Some threat actors put a lot of time and effort into infiltrating companies. It is common to set up look-alike websites and personas of vendors to add credibility to the ruse.

It is crucial to establish policies and procedures (Fundamental 9) to verify communications from vendors. Internal staff must be empowered to be extra vigilant and not blindly trust requests

that appear to come from a trusted partner. Staff that manage vendor relationships, especially financial aspects, should be immersed in advanced training regarding threat actor tactics.

Resource Links

- Recommended Practice: Improving Control System Cybersecurity with Defense-in-Depth Strategies (DHS NCCIC)
- Supply Chain Threats to Industrial Control: Third-Party Compromise (Dragos)
- Exposed and Vulnerable Critical Infrastructure: Water and Energy Industries (TrendMicro)
- Target Hackers Broke in Via HVAC Company (KrebsOnSecurity)
- NotPetya's Cost to FedEx: $400 Million and Counting (The Security Ledger)
- NotPetya attack totally destroyed Maersk's computer network: Chairman (SC Magazine)

14. Address All Smart Devices (IoT, IIoT, Mobile, etc.)

The proliferation of tablets, smartphones and other mobile devices, including the "internet of things" (IoT) and "industrial internet of things" (IIoT) in the workplace presents significant security challenges. Smart devices could present even greater risk to an organization than traditional computing devices if they are not securely configured and carefully managed.

Cisco's "2018 Annual Cybersecurity Report" states that few organizations view IoT as an imminent threat, yet adversaries are exploiting weaknesses in connected devices to gain access to industrial control systems that support critical infrastructure. The mobile, ubiquitous, and often inherently insecure nature of these devices means they are exposed to compromise from external applications, networks and malicious actors. The discoverability of these insecure and vulnerable internet-connected devices is trivial through the use of publicly available tools like Shodan and Censys.

Therefore, it is vital that all smart devices are included in the organizational risk management strategy – from asset inventory, supply chain and vulnerability management, to monitoring, policies and procedures, and everything in between. Furthermore, given the use of smart devices by employees to perform their jobs, it is imperative that safe and secure operation of these devices be included in training and awareness curriculum (Fundamental 8).

Industrial Internet of Things (IIoT)

While all connected devices need to be addressed, what is known as the industrial internet of things is of great concern to utilities. IIoT brings convenience and efficiency to water/wastewater management; it is the antithesis of air-gapped industrial deployments. Organizations simply cannot afford to deploy IIoT now and secure later, if at all. The cybersecurity risks and challenges brought about by IIoT cannot be ignored and must be addressed in the initial planning phases. To address IIoT concerns, the SANS Institute published a whitepaper, "2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns," to help organizations understand and manage the threats and risks associated with securing an IIoT infrastructure.

There is not one authoritative strategy to securing IIoT; however, several existing frameworks and methodologies can be used to drive IIoT security. Respondents to the 2018 SANS Industrial IoT Security Survey cited several sources, many used in concert, including NIST Cybersecurity Framework (CSF), NIST 800 series, IEEE, NIST Cyber-Physical Systems (CPS), NERC CIP and ENISA, to name a few.

IIoT Endpoints and Asset Inventory

Among top concerns of respondents from the 2018 SANS Industrial IoT Security Survey is the security of IIoT endpoints being the most vulnerable component of IIoT solutions. That makes asset inventory essential for IIoT, as insecure and vulnerable endpoints are likely directly connected to the internet both by design and by default configuration. Furthermore, many manufacturers' default configurations are widely known, published in user manuals, and publicly available on the internet for anyone to use.

IIoT and the Supply Chain

Currently there is no consistent standard prescribing how IIoT products are to be manufactured. The inconsistency leads to a variety of interoperability challenges among devices, as manufacturers often use proprietary protocols and vendor-specific implementations. This interoperability further confounds the security posture of IIoT devices and services. Therefore, along with asset inventory (Fundamental 1), it is equally imperative to assess all IIoT product and service providers through the supply chain risk management program (Fundamental 13).

A Word on Personal IoT Devices

Further contributing to the connected device challenge is the continued trend of employees using their personal electronic devices for work purposes (or in the work environment,) known as "bring your own device" or BYOD. Organizations need to address personal IoT devices in the workplace due to their potential for storing sensitive company data that could be used as a gateway into an organization, thus increasing the insider threat problem (Fundamental 12).

Resource Links

- Cybersecurity for Electronic Devices (DHS NCCIC)
- Guidelines for Managing the Security of Mobile Devices in the Enterprise - SP 800-124 (NIST)
- Mobile Device Security: Cloud and Hybrid Builds – SP 1800-4A (NIST)
- Baseline Security Recommendations for IoT - in the context of Critical Information Infrastructures (ENISA)
- Good practices for Security of Internet of Things in the context of Smart Manufacturing (ENISA)
- Industrial Internet Consortium (IIC)
- Water/Wastewater Utilities Leveraging IIoT (IIoT World)
- 2018 Annual Cybersecurity Report (Cisco)
- Internet of threats: Securing the Internet of Things for industrial and utility companies (IBM Institute for Business Value)

- IIoT World
- Shodan
- 7 Steps to Start Searching with Shodan (DARKReading)
- Censys
- 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns (SANS Institute) (membership required)

15. Participate in Information Sharing and Collaboration Communities

Participating in information sharing and collaboration communities is a soft cultural measure that is individually and collectively very potent. The more utilities engage and share with their regional peers and the community at-large, the more the sector benefits. Water and wastewater utilities and other critical infrastructure sectors all face the same cyber threats. Involvement with organizations that focus on cybersecurity and resilience enables the community to learn and share knowledge and experience to help one another.

WaterISAC is an excellent example of a place to share good ideas, successes, incident details and lessons learned. Other respected organizations with different strengths include the Multi-State ISAC; the Electricity ISAC; U.S. EPA's Water Security Division; national, regional, and state water and wastewater associations; InfraGard; and urban and regional law enforcement and intelligence fusion centers. We are stronger together.

One way to share with your peers is to develop case studies and presentations about challenges your utility has overcome. WaterISAC is always looking for content in the form of articles and webinar presentations. If you have a story to tell, or you just have a possible topic of interest to suggest, please get in touch with WaterISAC.

Roundtable discussions are ideal venues for peer-to-peer sharing and collaboration. For instance, a small group of utility IT and OT staff and managers in New England gather twice annually in an informal setting to discuss cybersecurity challenges and solutions. Participating in association conferences is another valuable sharing method. AWWA's annual Water Infrastructure Conference (WIC) offers numerous security and resilience presentations and opportunities to network with peers. Consider attending, or even presenting, at WIC or at events hosted by other associations.

Share Cybersecurity Incidents with WaterISAC

Reporting suspected or confirmed incidents is extremely valuable to the sector and, in many cases, national security. Reporting incidents helps WaterISAC and government security agencies learn which threats utilities are facing. This, in turn, influences the development of knowledge and resources to prevent future compromises and to assist with recovery and response.

Reporting IT and OT compromises also allow analysts to glean threat indicators from an incident. A type of threat intelligence, indicators of compromise are forensic data that can be used by network defenders to identify and block future attacks. They include virus signatures, malicious IP addresses, suspicious URLs and files – all artifacts that can signify potentially nefarious activity.

Refer to the section **Report Incidents and Suspicious Activity to WaterISAC and Authorities** in the beginning of this guide for more information about reporting incidents.

Resource Links:

- WaterISAC
- Multi-State ISAC
- Electricity ISAC
- U.S. EPA Water Security Division
- InfraGard
- National Fusion Center Association
- AWWA Water Infrastructure Conference