

Introduction to Cybersecurity Workshop Handouts



OCTOBER 2021



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

© 2019 WaterISAC

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

<i>Introduction</i>	<i>1</i>
<i>Report Incidents and Suspicious Activity to WaterISAC and Authorities</i>	<i>3</i>
<i>1. Perform Asset Inventories</i>	<i>7</i>
<i>2. Assess Risks</i>	<i>9</i>
<i>3. Minimize Control System Exposure.....</i>	<i>11</i>
<i>4. Enforce User Access Controls.....</i>	<i>15</i>
<i>5. Safeguard from Unauthorized Physical Access.....</i>	<i>19</i>
<i>6. Install Independent Cyber-Physical Safety Systems.....</i>	<i>21</i>
<i>7. Embrace Vulnerability Management.....</i>	<i>23</i>
<i>8. Create a Cybersecurity Culture</i>	<i>25</i>
<i>9. Develop and Enforce Cybersecurity Policies and Procedures (Governance)</i>	<i>29</i>
<i>10. Implement Threat Detection and Monitoring</i>	<i>31</i>
<i>11. Plan for Incidents, Emergencies and Disasters</i>	<i>35</i>
<i>12. Tackle Insider Threats</i>	<i>39</i>
<i>13. Secure the Supply Chain</i>	<i>41</i>
<i>14. Address All Smart Devices (IoT, IIoT, Mobile, etc.).....</i>	<i>43</i>
<i>15. Participate in Information Sharing and Collaboration Communities.....</i>	<i>47</i>

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 NRW 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](#)

Incident Action Checklist – Cybersecurity

For on-the-go convenience, the actions in this checklist are divided up into three “rip & run” sections and provide a list of activities that water and wastewater utilities can take to prepare for, respond to and recover from a cyber incident. You can also populate the “My Contacts” section with critical information that your utility may need during an incident.

Cyber Incidents and Water Utilities

Cyberspace and its underlying infrastructure are vulnerable to a wide range of hazards from both physical attacks as well as cyberthreats. Sophisticated cyber actors and nation-states exploit vulnerabilities to steal information and money and are developing capabilities to disrupt, destroy or threaten the delivery of essential services such as drinking water and wastewater.

As with any critical enterprise or corporation, drinking water and wastewater utilities must evaluate and mitigate their vulnerability to a cyber incident and minimize impacts in the event of a successful attack. Impacts to a utility may include, but are not limited to:

- Interruption of treatment, distribution or conveyance processes from opening and closing valves, overriding alarms or disabling pumps or other equipment
- Theft of customers’ personal data such as credit card information and social security numbers stored in on-line billing systems
- Defacement of the utility’s website or compromise of the email system
- Damage to system components
- Loss of use of industrial control systems (e.g., SCADA system) for remote monitoring of automated treatment and distribution processes



Cyber incidents can compromise the ability of water and wastewater utilities to provide clean and safe water to customers, erode customer confidence and result in financial and legal liabilities. The following sections outline actions drinking water and wastewater utilities can take to prepare for, respond to and recover from cyber incidents.



Actions to Prepare for a Cyber Incident



Utility

- ☐ Identify all mission critical information technology (IT) systems, considering business enterprise, process control and communications. Document the key functions of the mission critical objectives, and identify the personnel or entity responsible for operating and maintaining each IT system.
- ☐ Identify an overall IT security lead to coordinate with each IT system manager and oversee all cyber-related duties.
- ☐ Ensure that IT system managers enforce cybersecurity practices on all business enterprise, process control and communications systems. For example, verify adherence to user authentication, current anti-virus software and installation of security patches.
- ☐ Identify priority points of contact for reporting a cyber incident and requesting assistance with response and recovery. Include any state resources that may be available such as State Police, National Guard Cyber Division or mutual aid programs, as well as the Department of Homeland Security National Cybersecurity and Communications Integration Center (NCCIC) (888-282-0870 or NCCIC@hq.dhs.gov).
- ☐ Review and update the utility's emergency response plan (ERP) to address a cyber incident impacting business enterprise, process control and communications systems. Account for all potential impacts on operations, and ensure emergency contacts are current.
- ☐ Prevent unauthorized physical access to IT systems through security measures such as locks, sensors and alarms. Include workstations and process control systems (e.g., programmable logic controllers or PLCs).
- ☐ Train all essential personnel to perform mission critical functions during a cyber incident that disables business enterprise, process control and communications systems. Include the manual operation of water collection, storage, treatment and conveyance systems.
- ☐ Conduct drills and exercises for responding to a cyber incident that disables critical business enterprise, process control and communications systems.



Actions to Prepare for a Cyber Incident *(continued)*



IT Staff or Vendor

- ☐ Establish a program for maintaining updated anti-virus software on all critical IT systems, along with rapid installation of all security patches.
- ☐ Set up an automatic back-up on critical systems and ensure the process is producing a readable, uncorrupted restore file on a routine basis.
- ☐ Implement rigorous user authentication, including multi-factor authentication where possible. Use individual accounts and unique passwords for each employee, and restrict IT system access privileges to the level needed for a user's duties.
- ☐ Restrict internet access to process control systems unless absolutely necessary.
- ☐ Where possible, separate process control system traffic from business traffic through the use of a firewall. If this is not possible, logically filter traffic through the use of a firewall.
- ☐ Identify all routes of remote access to IT systems. Eliminate remote access where possible, and restrict remaining access (e.g., do not allow persistent remote access to control networks).
- ☐ Assess the use of additional strategies to protect IT systems, such as application whitelisting, network segmentation with restricted communication paths and active monitoring for adversarial system penetration.
- ☐ Conduct a detailed assessment of vulnerabilities in all mission critical IT systems. Consider use of the tools and subject matter experts provided by the DHS Industrial Control System Cyber Emergency Response Team (ICS-CERT) (www.ics-cert.us-cert.gov). Develop an action plan to mitigate all significant vulnerabilities identified in the assessment.

Notes:

Actions to Respond to a Cyber Incident



Utility

- ☐ If possible, disconnect compromised computers from the network to isolate breached components and prevent further damage, such as the spreading of malware. Do not turn off or reboot systems – this preserves evidence and allows for an assessment to be performed.
- ☐ Notify IT personnel and/or IT vendor of the incident and the need for emergency response assistance. In addition, NCCIC can assist with IT system response and recovery (888-282-0870 or NCCIC@hq.dhs.gov).
- ☐ Assess any damage to utility systems and equipment, along with disruptions to utility operations.
- ☐ Execute the utility ERP as needed, including notification of utility personnel, actions to restore operations of mission critical processes (e.g., switch to manual operation if necessary), and public notification (if required).
- ☐ Report the cyber incident as required to law enforcement and regulatory agencies.
- ☐ Notify any external entities (e.g., vendors, other government offices) that may have remote connections to the affected network(s).
- ☐ Document key information on the incident, including any suspicious calls, emails, or messages before or during the incident, damage to utility systems, and steps taken in response to the incident (including dates and times).

IT Staff or Vendor

- ☐ Review system and network logs, and use virus and malware scans to identify affected equipment, systems, accounts and networks.
- ☐ Document which user accounts were or are logged on, which programs and processes were or are running, any remote connections to the affected IT systems or network(s) and all open ports and their associated applications.
- ☐ If possible, take a “forensic image” of the affected IT systems to preserve evidence. Tools to take forensic images include Forensic Tool Kit (FTK) and EnCase.
- ☐ If possible, identify any malware used in the incident, any remote servers to which data may have been sent during the incident, and the origin of the incident. NCCIC can assist with the forensic analysis (888-282-0870 or NCCIC@hq.dhs.gov).
- ☐ Research and identify if any employee or customer personally identifiable information (PII) was compromised.
- ☐ Check the system back-up time stamp to determine if the back-up was compromised during the incident.
- ☐ Document all findings, and avoid modifying or deleting any data that might be attributable to the incident.

Notes:

Actions to Recover from a Cyber Incident



Utility

- ☐ Continue to work with IT staff, vendors and integrators, government partners and others to obtain needed resources and assistance for recovery.
- ☐ Notify affected employees and customers if any PII was compromised.
- ☐ Submit an incident report through WaterISAC (866-H2O-ISAC). Membership is not required to submit a report.
- ☐ Develop a lessons learned document and/or an after action report (AAR) to document utility response activities, successes, and areas for improvement. Create an improvement plan (IP) based on your AAR and use the IP to update your vulnerability assessment, ERP and contingency plans.
- ☐ Register for cybersecurity alerts and advisories from water sector and government partners to be aware of new vulnerabilities and threats. Two sources of cybersecurity alerts are WaterISAC, which has a basic membership that is free, and ICS-CERT (<https://ics-cert.us-cert.gov/alerts>).

IT Staff or Vendor

- ☐ Remove any malware, corrupted files and other changes made to IT systems by the incident.
- ☐ Restore IT systems as required (e.g., re-image hard drives, reload software). NCCIC can assist with the IT system recovery (888-282-0870 or NCCIC@hq.dhs.gov).
- ☐ Restore compromised files from a system back-up that has not been compromised.
- ☐ Install patches and updates, disable unused services and perform other countermeasures to harden the system against known vulnerabilities that may have been exploited.

Notes:

My Contacts and Resources



CONTACT NAME	UTILITY/ORGANIZATION NAME	PHONE NUMBER
	Law Enforcement	
	IT Staff/Vendor	
	SCADA Staff/Vendor	
	DHS NCCIC	888-282-0870
	Local Laboratory	
	State Primacy Agency	
	Local Emergency Management Agency	
	Local Health Department	
	WARN Chair	
	State Emergency Management Agency	

Resources

- [Best Cybersecurity Practices](#) (WaterISAC)
- [Cyber Security Evaluation Tool](#) (DHS ICS-CERT)
- [Advisories](#) (DHS ICS-CERT)
- [Cybersecurity Advisors](#) (DHS)
- [National Cybersecurity and Communications Integration Center \(NCCIC\)](#) (DHS)
- Cybersecurity Guidance and Tool (AWWA)
- Cybersecurity Resource Guide (WaterISAC)
- Cybersecurity Insurance (National Rural Water Association)

Notes:



WATER SECTOR CYBERSECURITY BRIEF FOR STATES

Introduction

Implementing cybersecurity best practices is critical for water and wastewater utilities. Cyber-attacks are a growing threat to critical infrastructure sectors, including water and wastewater systems. Many critical infrastructure facilities have experienced cybersecurity incidents that led to the disruption of a business process or critical operation.

Cyber Threats to Water and Wastewater Systems

Cyber-attacks on water or wastewater utility business enterprise or process control systems can cause significant harm, such as:

- Upset treatment and conveyance processes by opening and closing valves, overriding alarms or disabling pumps or other equipment;
- Deface the utility's website or compromise the email system;
- Steal customers' personal data or credit card information from the utility's billing system; and
- Install malicious programs like ransomware, which can disable business enterprise or process control operations.

These attacks can: compromise the ability of water and wastewater utilities to provide clean and safe water to customers, erode customer confidence, and result in financial and legal liabilities.

Benefits of a Cybersecurity Program

The good news is that cybersecurity best practices can be very effective in eliminating the vulnerabilities that cyber-attacks exploit. Implementing a basic cybersecurity program can:

- Ensure the integrity of process control systems;
- Protect sensitive utility and customer information;
- Reduce legal liabilities if customer or employee personal information is stolen; and
- Maintain customer confidence.

Challenges for Utilities in Starting a Cybersecurity Program

Many water and wastewater utilities, particularly small systems, lack the resources for information technology (IT) and security specialists to assist them with starting a cybersecurity program. Utility personnel may believe that cyber-attacks do not present a risk to their systems or feel that they lack the technical capability to improve their cybersecurity.

Be assured, however, that basic cybersecurity best practices can be carried out by utility personnel without specialized training, and user-friendly resources are available to help. You just have to know how to start and where to look!



WATER SECTOR CYBERSECURITY BRIEF FOR STATES

How to Use This Brief

EPA developed this brief in cooperation with the Association of State Drinking Water Administrators' Security Committee to help state staff (or their designated assistance providers) start a conversation with utilities about cybersecurity. Information gathered from the questions on this page can help you to understand a utility's current cybersecurity practices and point them toward resources to enhance their program. You may also leave the next two pages with the utility as a reminder of your discussions. Those pages provide recommendations for building a cybersecurity program and responding to cyber-attacks.

10 Questions for a Cybersecurity Dialogue with a Utility*

Does your utility ...

1. **Keep an inventory of control system devices and ensure this equipment is not exposed to networks outside the utility?**
 - Never allow any machine on the control network to “talk” directly to a machine on the business network or on the Internet.
2. **Segregate networks and apply firewalls?**
 - Classify IT assets, data, and personnel into specific groups, and restrict access to these groups.
3. **Use secure remote access methods?**
 - A secure method, like a virtual private network, should be used if remote access is required.
4. **Establish roles to control access to different networks and log system users?**
 - Role-based controls will grant or deny access to network resources based on job functions.
5. **Require strong passwords and password management practices?**
 - Use strong passwords and have different passwords for different accounts.
6. **Stay aware of vulnerabilities and implement patches and updates when needed?**
 - Monitor for and apply IT system patches and updates.
7. **Enforce policies for the security of mobile devices?**
 - Limit the use of mobile devices on your networks and ensure devices are password protected.
8. **Have an employee cybersecurity training program?**
 - All employees should receive regular cybersecurity training.
9. **Involve utility executives in cybersecurity?**
 - Organizational leaders are often unaware of cybersecurity threats and needs.
10. **Monitor for network intrusions and have a plan in place to respond?**
 - Be capable of detecting a compromise quickly and executing an incident response plan.
11. For more information about each of these questions, see *WaterISAC 15 Cybersecurity Fundamentals for Water and Wastewater Utilities* at <https://www.waterisac.org/fundamentals>.

Taking the Next Step with a Utility

If utility staff can knock each of these questions/answers out of the park, then the utility has a good cybersecurity program in place. However, if the response to these questions is “No,” “Not sure,” or “How about this weather?” then encourage the utility to use the next page to start building a cybersecurity program.



IMPLEMENTING A CYBERSECURITY PROGRAM AT YOUR WATER OR WASTEWATER UTILITY

Cybersecurity Worksheet

Use this worksheet as recommendations for an effective cybersecurity program. Talk to your IT service providers and others who manage your IT systems about how to carry out these actions at your utility.

Action	Notes	Date Completed
Audit IT systems and identify vulnerabilities		
Keep a list of the highest cybersecurity risks and how they will be addressed		
Ensure all IT systems have up-to-date antivirus and anti-malware software		
Install security patches on all IT systems on a monthly basis		
Implement secure remote access practices		
Segregate networks and control access to networks based on job function		
Monitor networks for suspicious activity and be prepared to respond if detected		
Establish strong password policies		
Consider “application whitelisting” on critical systems (allow execution of approved files only)		
Improve physical security for IT equipment		
Segregate business enterprise and process control systems, and require separate credentials for access		
Establish secure policies for mobile devices		
Develop a contingency and disaster recovery plan for critical IT systems		
Develop and exercise SOPs for manual operation of utility processes if control systems are compromised		
Implement redundancies in your system to limit service outages		
Conduct cybersecurity training for utility staff and contractors		



IMPLEMENTING A CYBERSECURITY PROGRAM AT YOUR WATER OR WASTEWATER UTILITY

Steps for Responding to a Suspected Cyber Incident at a Water or Wastewater Utility

Response

1. Disconnect compromised computers from the network. Do *not* turn off or reboot systems.
2. Assess the scope of the compromise, and isolate all affected IT systems.
3. Open a ticket with your antivirus software or security service vendor.
4. Assess any potential damage, including impacts to treatment processes or service disruptions.
5. Initiate manual operation of equipment if control systems have been compromised.
6. Distribute any advisories or alerts to customers as needed, including customers whose records may have been compromised.
7. Identify methods to scan all IT assets to eradicate malicious code. Assess and implement recovery procedures.

Reporting

1. Report the incident to local law enforcement and the primary oversight agency (typically, the state).
2. Contact the DHS Cybersecurity and Infrastructure Security Agency (CISA) at <https://www.cisa.gov/reporting-cyber-incidents>. CISA can assist your utility with identifying and restoring affected systems, coordinating federal assistance, and improving security.
3. Submit an incident report through [WaterISAC](https://www.waterisac.org) (analyst@waterisac.org; 866-H2O-ISAC).

Important Contact Information

Role	Point of Contact	Phone Number	Email
IT service vendor			
Local law enforcement			
State agency			
Cybersecurity and Infrastructure Security Agency (CISA)			https://www.cisa.gov/reporting-cyber-incidents
WaterISAC		866-H2O-ISAC	analyst@waterisac.org

For More Information

For more information on available cybersecurity guidance and resources:

- [WaterISAC 15 Cybersecurity Fundamentals for Water and Wastewater Utilities](#)
- [DHS Cybersecurity and Infrastructure Security Agency](#)
- [American Water Works Association \(AWWA\) Resources on Cybersecurity](#)
- [EPA Cybersecurity Incident Action Checklist](#)



Cyber Incident Reporting

A Unified Message for Reporting to the Federal Government

Cyber incidents can have serious consequences. The theft of private, financial, or other sensitive data and cyber attacks that damage computer systems are capable of causing lasting harm to anyone engaged in personal or commercial online transactions. Such risks are increasingly faced by businesses, consumers, and all other users of the Internet.

A private sector entity that is a victim of a cyber incident can receive assistance from government agencies, which are prepared to investigate the incident, mitigate its consequences, and help prevent future incidents. For example, federal law enforcement agencies have highly trained investigators who specialize in responding to cyber incidents for the express purpose of disrupting threat actors who caused the incident and preventing harm to other potential victims. In addition to law enforcement, other federal responders provide technical assistance to protect assets, mitigate vulnerabilities, and offer on-scene response personnel to aid in incident recovery. When supporting affected entities, the various agencies of the Federal Government work in tandem to leverage their collective response expertise, apply their knowledge of cyber threats, preserve key evidence, and use their combined authorities and capabilities both to minimize asset vulnerability and bring malicious actors to justice. This fact sheet explains when, what, and how to report to the Federal Government in the event of a cyber incident.

When to Report to the Federal Government

A cyber incident is an event that could jeopardize the confidentiality, integrity, or availability of digital information or information systems. Cyber incidents resulting in significant damage are of particular concern to the Federal Government. Accordingly, victims are encouraged to report all cyber incidents that may:

- result in a significant loss of data, system availability, or control of systems;
- impact a large number of victims;
- indicate unauthorized access to, or malicious software present on, critical information technology systems;
- affect critical infrastructure or core government functions; or
- impact national security, economic security, or public health and safety.

What to Report

A cyber incident may be reported at various stages, even when complete information may not be available. Helpful information could include who you are, who experienced the incident, what sort of incident occurred, how and when the incident was initially detected, what response actions have already been taken, and who has been notified.

How to Report Cyber Incidents to the Federal Government

Private sector entities experiencing cyber incidents are encouraged to report a cyber incident to the local field offices of federal law enforcement agencies, their sector specific agency, and any of the federal agencies listed in the table on page two. The federal agency receiving the initial report will coordinate with other relevant federal stakeholders in responding to the incident. If the affected entity is obligated by law or contract to report a cyber incident, the entity should comply with that obligation in addition to voluntarily reporting the incident to an appropriate federal point of contact.

Types of Federal Incident Response

Upon receiving a report of a cyber incident, the Federal Government will promptly focus its efforts on two activities: Threat Response and Asset Response. Threat response includes attributing, pursuing, and disrupting malicious cyber actors and malicious cyber activity. It includes conducting criminal investigations and other actions to counter the malicious cyber activity. Asset response includes protecting assets and mitigating vulnerabilities in the face of malicious cyber activity. It includes reducing the impact to



systems and/or data; strengthening, recovering and restoring services; identifying other entities at risk; and assessing potential risk to the broader community.

Irrespective of the type of incident or its corresponding response, Federal agencies work together to help affected entities understand the incident, link related incidents, and share information to rapidly resolve the situation in a manner that protects privacy and civil liberties.

Key Federal Points of Contact	
Threat Response	Asset Response
<p>Federal Bureau of Investigation (FBI)</p> <p>FBI Field Office Cyber Task Forces: http://www.fbi.gov/contact-us/field</p> <p>Internet Crime Complaint Center (IC3): http://www.ic3.gov</p> <p><i>Report cybercrime, including computer intrusions or attacks, fraud, intellectual property theft, identity theft, theft of trade secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity to FBI Field Office Cyber Task Forces.</i></p> <p><i>Report individual instances of cybercrime to the IC3, which accepts Internet crime complaints from both victim and third parties.</i></p>	<p>National Cybersecurity and Communications Integration Center (NCCIC)</p> <p>NCCIC: (888) 282-0870 or NCCIC@hq.dhs.gov</p> <p>United States Computer Emergency Readiness Team: http://www.us-cert.gov</p> <p><i>Report suspected or confirmed cyber incidents, including when the affected entity may be interested in government assistance in removing the adversary, restoring operations, and recommending ways to further improve security.</i></p>
<p>National Cyber Investigative Joint Task Force</p> <p>NCIJTF CyWatch 24/7 Command Center: (855) 292-3937 or cywatch@ic.fbi.gov</p> <p><i>Report cyber intrusions and major cybercrimes that require assessment for action, investigation, and engagement with local field offices of federal law enforcement agencies or the Federal Government.</i></p>	
<p>United States Secret Service</p> <p>Secret Service Field Offices and Electronic Crimes Task Forces (ECTFs): http://www.secretservice.gov/contact/field-offices</p> <p><i>Report cybercrime, including computer intrusions or attacks, transmission of malicious code, password trafficking, or theft of payment card or other financial payment information</i></p>	
<p>United States Immigration and Customs Enforcement / Homeland Security Investigations (ICE/HSI)</p> <p>HSI Tip Line: 866-DHS-2-ICE (866-347-2423) or https://www.ice.gov/webform/hsi-tip-form</p> <p>HSI Field Offices: https://www.ice.gov/contact/hsi</p> <p>HSI Cyber Crimes Center: https://www.ice.gov/cyber-crimes</p> <p><i>Report cyber-enabled crime, including: digital theft of intellectual property; illicit e-commerce (including hidden marketplaces); Internet-facilitated proliferation of arms and strategic technology; child pornography; and cyber-enabled smuggling and money laundering.</i></p>	
If there is an immediate threat to public health or safety, the public should always call 911.	

CYBERSECURITY ADVISORS

THE CYBERSECURITY AND INFRASTRUCTURE AGENCY'S (CISA) CYBERSECURITY ADVISOR (CSA) PROGRAM OFFERS CYBERSECURITY ASSISTANCE ON A VOLUNTARY, NO-COST BASIS TO CRITICAL INFRASTRUCTURE ORGANIZATIONS, TO INCLUDE STATE, LOCAL, TRIBAL, AND TERRITORIAL (SLTT) GOVERNMENTS. THROUGH THE CSA PROGRAM, YOUR ORGANIZATION CAN PREPARE FOR AND PROTECT AGAINST CYBERSECURITY THREATS TO CRITICAL INFRASTRUCTURE.

GOALS

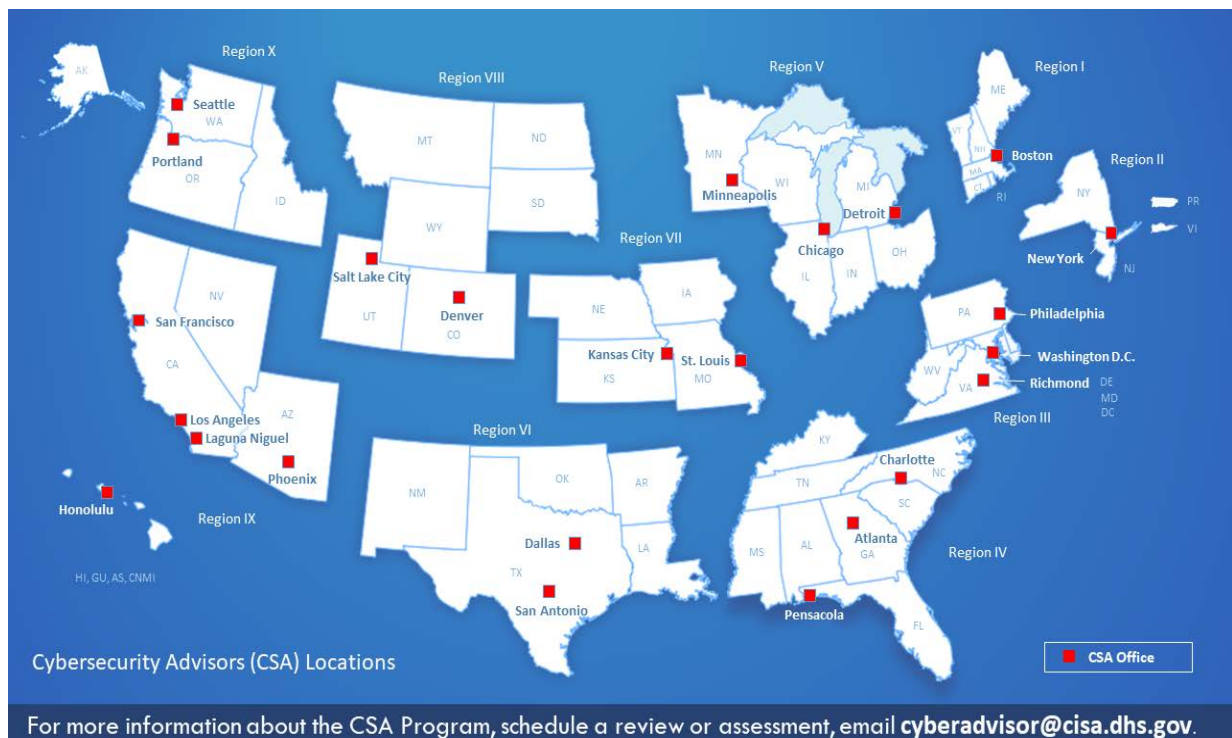
The goal of the CSA program is to promote cybersecurity preparedness, risk mitigation, and incident response capabilities of public and private sector owners and operators of critical infrastructure, as well as SLTT bodies, through stakeholder partnerships and direct assistance activities.

APPROACH

The CSA program maintains regional subject matter experts throughout DHS emergency management and protection regions. Regional CSAs cultivate partnerships with participating organizations and initiate information sharing. CSAs introduce organizations to various no-cost DHS cybersecurity products and services, along with other public and private resources, and act as liaisons to other DHS cyber programs and leadership. CSAs also collaborate with local and federal entities to facilitate delivery of cybersecurity services across the United States.

Service	What CSAs Offer	What Value Our Partners Receive
Cyber Preparedness	On-site preparedness and protective visits, work- shops, and engaging activities	Cybersecurity ideas, advice, and best practices and a formal exchange to raise awareness of DHS cybersecurity products, services, and information resources relative to critical infrastructure and partnerships
Strategic Messaging	DHS cybersecurity briefings, keynote addresses, and panel discussions	Improved cybersecurity awareness and collaboration potential, to convey timely and relevant information on DHS programs and operational activities
Working Group Support	Leadership at existing forums and working groups, engaging stakeholders with in-place cybersecurity initiatives and information sharing groups	Improved coordination with DHS on cybersecurity policy, procedures, and best practices; and an opportunity to exchange lessons-learned and identify areas of mutual interest
Partnership Development	Engagements to develop, build capacity in, and strengthen private-public cybersecurity partner- ships	Help initiating cybersecurity partnerships, establishing charter objectives and milestones, and maturing local and regional cybersecurity posture — in order to move partnerships from awareness building to operational capabilities

Cyber Assessments	Cyber Infrastructure Survey (CIS)	Assessment of more than 80 cybersecurity controls in five domains: cybersecurity management, cybersecurity forces, cybersecurity controls, cyber incident response, and cyber dependencies, resulting in an interactive decision support tool
	Cyber Resilience Review (CRR)	Assessment of cybersecurity management capabilities and maturity aspects of an organization's critical information technology (IT) services and associated assets — and in the context of the NIST Cybersecurity Framework (CSF)
	External Dependency Management (EDM)	Assessments of management activities and practices used to identify, analyze, and reduce risks arising from third parties
Incident Coordination and Support	Direct assistance and resourcing support, conducted in times of cyber threat, disruption, and attack	Facilitated cyber incident response and resource coordination, information de-confliction, and information request assistance



CYBER RESILIENCE REVIEW

THE PRESIDENTIAL POLICY DIRECTIVE (PPD) 41, UNITED STATES CYBER INCIDENT COORDINATION, SETS FORTH THE PRINCIPLES GOVERNING THE FEDERAL GOVERNMENT'S RESPONSE TO CYBER INCIDENTS AND ESTABLISHES LEAD AGENCIES AND PLANS FOR COORDINATING THE BROADER FEDERAL GOVERNMENT RESPONSE FOR THE AFFECTED ENTITIES, OR VICTIMS, OF SUCH INCIDENTS.



FORMAT AND GOAL

CISA offers two options for the CRR: a downloadable self-assessment and a facilitated six-hour session with trained DHS representatives at your locations.

Through the CRR, the organization will develop an understanding of its operational resilience and ability to manage cyber risk during normal operations and times of operational stress and crisis.



APPROACH

The CRR is derived from the CERT Resilience Management Model (CERT-RMM), a process improvement model developed by Carnegie Mellon University's Software Engineering Institute for managing operational resilience. The CRR is based on the premise that an organization deploys its assets (people, information, technology, and facilities) to support specific critical services or products. Based on this principle, the CRR evaluates the maturity of your organization's capacities and capabilities in performing, planning, managing, measuring and defining cybersecurity capabilities across 10 domains:

- Asset Management,
- Controls Management,
- Configuration and Change Management,
- Vulnerability Management,
- Incident Management,
- Service Continuity Management,
- Risk Management,
- External Dependencies Management,
- Training and Awareness, and
- Situational Awareness.



PARTICIPANTS

To conduct a CRR, CISA recommends that you involve a cross-functional team representing business, operations, security, information technology, and maintenance areas, including those responsible for the functions below:

- IT policy and governance (e.g., Chief Information Security Officer)
- IT security planning and management (e.g., Director of Information Technology)
- IT infrastructure (e.g., network/system administrator)

- IT operations (e.g., configuration/change managers)
- Business operations (e.g., operations manager)
- Business continuity and disaster recovery planning (e.g., BC/DR manager)
- Risk management (e.g., enterprise/operations risk manager)
- Procurement and vendor management (e.g., contracts and legal support managers)

BENEFITS AND OUTCOMES

The CRR provides a better understanding of an organization's cybersecurity posture. The review provides an improved organization-wide awareness of the need for effective cybersecurity management; a review of capabilities most important to ensuring the continuity of critical services during times of operational stress and crisis; a verification of management success; a catalyst for dialog between participants from different functional areas within your organization; and a comprehensive final report that maps the relative maturity of the organizational resilience processes in each of the 10 domains, and that includes improvement options for consideration, using recognized standards and best practices as well as references to the CERTRMM.

DATA PRIVACY

The CRR report is created exclusively for your organization's internal use. All data collected and analysis performed during a CRR assessment is afforded protection under the DHS Protected Critical Infrastructure Information (PCII) Program. PCII program protection means that DHS employees are trained in the safeguarding and handling of PCII, DHS cannot publicly disclose PCII, and PCII cannot be used for regulatory purposes. To learn more, please visit www.dhs.gov/pcii.

ASSOCIATION TO THE CYBERSECURITY FRAMEWORK

The principles and recommended practices within the CRR align with the Cybersecurity Framework (CSF) developed by the National Institute of Standards and Technology (NIST). After performing a CRR, your organization can compare the results to the criteria of the NIST CSF to identify gaps and, where appropriate, recommended improvement efforts. A reference crosswalk mapping the relationship of the CRR goals and practices to the NIST CSF categories and subcategories is included in the CRR self-assessment kit. An organization's assessment of CRR practices and capabilities may or may not indicate that the organization is fully aligned to the NIST CSF.

CYBER INFRASTRUCTURE SURVEY

THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA) OFFERS THE CYBER INFRASTRUCTURE SURVEY (CIS) ON A VOLUNTARY, NO-COST BASIS FOR CRITICAL INFRASTRUCTURE ORGANIZATIONS AND STATE, LOCAL, TRIBAL, AND TERRITORIAL GOVERNMENTS. ADMINISTERED BY REGIONALLY-LOCATION CYBERSECURITY ADVISORS, A CIS EVALUATES THE EFFECTIVENESS, RESILIENCE AND CYBERSECURITY PREPAREDNESS OF AN ORGANIZATION'S SECURITY CONTROLS.

FORMAT AND GOAL

A CIS is a facilitated, expert-led assessment with cybersecurity personnel from your organization (e.g., Chief Information Security Officer, ICS/SCADA Security Manager, IT Security Manager). This informal interview typically takes 2½ to 4 hours in length. Its goal is to assess the foundational and essential cybersecurity practices of an organization's critical service to identify dependencies, capabilities and emerging effects of the current cybersecurity posture. After the survey, DHS will provide an interactive dashboard for scenario planning.

APPROACH

CIS focuses on a service-based-view versus a programmatic-view of cybersecurity. Critical services are assessed against more than 80 cybersecurity controls grouped under five top-level domains: cybersecurity management, cybersecurity forces, cybersecurity controls, cyber incident response, and cyber dependencies.

Following the assessment, DHS will provide a user friendly dashboard for reviewing and interacting with the survey findings. Your organization can use the dashboard to compare its results against its industry peers, review results in the context of specific cyber and physical threat scenarios, and dynamically adjust the importance of in-place practices to see the effects on overall cyber protection.

CYBERSECURITY FRAMEWORK

The cybersecurity controls surveyed within the CIS broadly align to the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF), but does not show an organization's adherence to the NIST CSF. The CIS computes a unique, service-specific cyber protective resilience index based on only a narrow set of cyber protection and resilience measures. The NIST CSF is a comprehensive framework and should be considered as a next step after leveraging the CIS results.

BENEFITS AND OUTCOMES

A CIS provides your organization with:

- * An effective assessment of cybersecurity controls in-place for critical service;
 - * A user friendly, interactive dashboard to support cybersecurity planning and resource allocation; and
 - * Access to peer performance data, visually depicted on the dashboard.
-



DATA PRIVACY

The CIS dashboard is for your organization's exclusive use. All data collected and analysis performed during the CIS is afforded protection under the DHS Protected Critical Infrastructure Information (PCII) Program. PCII program protection means that DHS employees are trained in the safeguarding and handling of PCII, DHS cannot publicly disclose PCII, and PCII cannot be used for regulatory purposes. To learn more, please visit www.dhs.gov/pcii.



CIS Survey Question Domains

CIS Domains

Cybersecurity Forces

- * Personnel
- * Cybersecurity Training

Cybersecurity Controls

- * Authentication and Authorization Controls
- * Access Controls
- * Cybersecurity Measures
- * Information Protection
- * User Training
- * Defense Sophistication and Compensating Controls

Incident Response

- * Incident Response Measures
- * Alternate Site and Disaster Recovery

Cybersecurity Management

- * Cybersecurity Leadership
- * Cyber Service Architecture

- * Change Management
- * Lifecycle Tracking
- * Assessment and Evaluation
- * Cybersecurity Plan
- * Cybersecurity Exercises
- * Information Sharing


Dependencies

- * Data at Rest
- * Data in Motion
- * Data in Process
- * End Point Systems

EXTERNAL DEPENDENCIES MANAGEMENT ASSESSMENT

THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA) OFFERS THE EXTERNAL DEPENDENCIES MANAGEMENT (EDM) ASSESSMENT ON A VOLUNTARY, NO-COST BASIS FOR CRITICAL INFRASTRUCTURE ORGANIZATIONS AND STATE, LOCAL, TRIBAL, AND TERRITORIAL GOVERNMENTS. ADMINISTERED BY REGIONALLY-LOCATED CYBERSECURITY ADVISORS, THE ASSESSMENT PROVIDES AN ORGANIZATION WITH A BETTER UNDERSTANDING OF HOW THEY MANAGE RISKS ARISING FROM DEPENDENCES ON THE INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) SUPPLY CHAIN.

FORMAT AND GOALS




The EDM Assessment is conducted as a four-hour session at a location of your choosing and facilitated by trained DHS representatives. Your organization can use the assessment by itself and as the first step in an improvement effort. You also may use it in conjunction with CISA's External Dependencies Management Method, which provides a rigorous, repeatable way to identify and manage specific suppliers or other external entities that your organization depends on to support its mission.

The goals of the assessment are to:

- Evaluate the activities and practices your organization uses to manage risks arising from external dependencies.
- Provide an objective review of your organization's capabilities in the assessed areas and recommendations offering a roadmap for improvement based on industry-leading practices.

APPROACH



Risks associated with the ICT supply chain have grown dramatically with expanded outsourcing of technology and infrastructure. Failures in managing these risks have resulted in incidents affecting millions of people.

The EDM Assessment focuses on the relationship between your organization's high-value services and assets (people, technology, facilities, and information) and evaluates how you manage risks incurred from using the ICT supply chain to support these high-value services. The ICT supply chain consists of outside parties that operate, provide, or support information and communications technology. Common examples include externally provided web and data hosting, telecommunications services, and data centers, as well as any service that depends on the secure use of ICT.

Through the EDM Assessment, your organization will evaluate:

- Relationship Formation – how your organization considers third-party risks, selects external entities, and forms relationships with them so that risk is managed from the start.
- Relationship Management and Governance – how your organization manages ongoing relationships with external entities to support and strengthen your critical services at a managed level of risk and costs.

- Service Protection and Sustainment – how your organization plans for, anticipates, and manages disruption or incidents related to external entities.

The EDM Assessment evolved from the DHS Cyber Resilience Review (CRR) and, like the CRR, is based on the CERT Resilience Management Model (CERT-RMM), a process improvement model developed by Carnegie Mellon University's Software Engineering Institute.

BENEFITS AND OUTCOMES

Through an EDM Assessment, your organization will gain a better understanding of your cybersecurity posture relating to external dependencies. The assessment provides:

- An opportunity for participants from different parts of your organization to discuss issues relating to vendors and reliance on external entities;
- Options for consideration that guide improvement efforts, using recognized standards and best practices drawn from such sources as the CERT-RMM, NIST standards, and the NIST Cybersecurity Framework; and
- A comprehensive report on your third-party risk management practices and capabilities.

DATA PRIVACY

The EDM Assessment report is created exclusively for your organization's internal use. All data collected and analysis performed during an EDM assessment is afforded protection under the CISA Protected Critical Infrastructure Information (PCII) Program. PCII program protection means that CISA employees are trained in the safeguarding and handling of PCII, CISA cannot publicly disclose PCII, and PCII cannot be used for regulatory purposes. To learn more, please visit www.dhs.gov/pcii.

PARTICIPANTS

To conduct an EDM assessment, CISA recommends that you involve a cross-functional team that includes those responsible for the functions shown in the following.

- IT security planning and management (e.g., Director of Information Technology)
- IT operations (e.g., configuration/change managers)
- Risk managers, in particular operations risk (e.g., enterprise/operations risk manager)
- Business continuity and disaster recovery planning (e.g., BC/DR manager)
- IT policy and governance (e.g., Chief Information Security Officer)
- Business management (e.g., operations manager)
- Procurement and vendor management (e.g., contracts and legal support managers)
- Legal

CYBER RESILIENCE WORKSHOP

THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY'S (CISA) CYBERSECURITY ADVISOR (CSA) PROGRAM OFFERS CYBER RESILIENCE WORKSHOPS ON A VOLUNTARY, NO-COST BASIS FOR CRITICAL INFRASTRUCTURE ORGANIZATIONS, TO INCLUDE STATE, LOCAL, TRIBAL, AND TERRITORIAL GOVERNMENTS. THROUGH THE WORKSHOP, YOUR ORGANIZATION WILL BE INTRODUCED TO CYBER RESILIENCE CONCEPTS AND WAYS TO IMPROVE MANAGEMENT OF CYBER RESILIENCE.

FORMAT



The Cyber Resilience Workshop is a four-hour collaborative session led by CISA representatives. Each workshop is tailored to the concerns and threats of a specific sector and provides an opportunity for professionals to learn together. Workshops are held on demand (based on availability) at locations convenient to participants.

GOAL



The goal of the workshop is to provide your organization with tangible, useful take-away information related to risk-based decision making and security planning for critical services.

APPROACH



Through the workshop, your organization will be introduced to cyber resilience concepts and capability-building activities in key performance areas such as cybersecurity, IT operations, and business continuity. The workshop will address both operational risk management and emergency/crisis management. Structured drills and scenarios will help your organization examine capability building in operational resilience practices, going well beyond discussions of IT security controls and countermeasures. Content and threat examples specific to your sector or industry will be emphasized.

PARTICIPANTS



CISA recommends that a cross-functional team from your organization's business and operations attend the workshop, including those responsible for the functions below:

- IT policy and governance (e.g., Chief Information Security Officer)
- IT security planning and management (e.g., Director of Information Technology)
- IT infrastructure (e.g., network/system administrator)
- IT operations (e.g., configuration/change managers)
- Business operations (e.g., operations manager)
- Business continuity and disaster recovery planning (e.g., BC/DR manager)
- Risk management (e.g., enterprise/operations risk manager)
- Procurement and vendor management (e.g., contracts and legal support managers)



BENEFITS AND OUTCOMES

The Cyber Resilience Workshop is designed to keep communities-of-interest informed on national cybersecurity, policies, initiatives, and federal capabilities, and to encourage working partnerships with these communities on matters of cybersecurity. The workshop will provide your organization with a greater awareness of:

- Federal initiatives affecting critical infrastructure protection and realistic practices for improving operational resilience;
- Gaps in cyber management practices and potential process improvements;
- Cybersecurity best practices and operational resilience concepts;
- Processes to maintain and repeatedly carry out protection and sustainment activities for critical assets and services;
- Ways to enhance cyber incident response and business continuity capabilities; and
- Federal coordination for incident notification, containment, and recovery.



FOR INFORMATION AND SCHEDULING

The Cyber Resilience Workshop is facilitated by regional personnel of the Cybersecurity Advisor (CSA) Program. Email cyberadvisor@hq.dhs.gov for more information on the Cyber Resilience Workshop and on the schedules and locations of upcoming sessions.



CISA
CYBER+INFRASTRUCTURE

DEFEND TODAY. SECURE TOMORROW.

CYBERSECURITY ASSESSMENTS SUMMARY

Name	Cyber Resilience Review (CRR)	External Dependency Management (EDM)	Cyber Infrastructure Survey (CIS)	Onsite Cyber Security Evaluation Tool (CSET)
Purpose and Value Proposition	Identifies and evaluates cyber security management capabilities, maturity, and capacity to manage cyber risk during normal operations and times of operational stress.	Assesses the activities and practices utilized by an organization to manage risks arising from external dependencies.	Identifies cybersecurity controls and protective measures in place and provides an interactive dashboard for comparative analysis and valuation.	Provides a detailed, effective, and repeatable tool for assessing systems security against established industry standards and guidance
Scope	Critical Service view	Critical Service view	Critical Service view	Information Technology and Operational Technology systems
Time to Execute/	5 to 6 Hours	3 – 4 Hours	2 ½ to 4 Hours	Varies greatly (min 2 Hours) (self-assessment)
Information Sought	Capabilities and maturity indicators in 10 security domains	Capabilities and maturity indicators across third party relationship management lifecycle domains	Protective measures in-place	Architecture diagrams, infrastructure, policies, and procedures documents
Preparation	Planning call to scope evaluation	Planning call to scope evaluation	Planning call to scope evaluation	Self-assessment available from web site and utilized locally
Participants	IT/Security Manager, Continuity Planner, and Incident Responders	IT/Security Manager, Continuity Planner, with Contract Management	IT/Security Manager	Operators, engineers, IT staff, policy/ management personnel, and subject matter experts
All Assessments Delivered By	Contact the Cybersecurity Advisor mailbox at cyberadvisor@hq.dhs.gov for more information or to request services			

CISA ASSESSMENTS

The CISA Assessments team supports Federal, State, Local, Tribal and Territorial Governments and Critical Infrastructure partners by providing proactive testing and assessment services. The team also provides an objective third-party perspective of stakeholder operational cybersecurity posture and identifies security control strengths and weaknesses. CISA Assessments aggregates these insights into actionable reports that champion the implementation of mitigations and controls capable of positive impact toward overall risk reduction.



OBJECTIVES

- Reduce Stakeholder Risk
- Enable Data-Driven Decision
- Influence Operational Behaviors
- Increase National Resilience



SERVICE OFFERINGS

- **Vulnerability Scanning** is the persistent scanning of internet-accessible systems for vulnerabilities, configuration errors, and suboptimal security practices.
- **Phishing Campaign Assessments** measure propensity to click on email phishing lures which increases organizational training and awareness.
- **Remote Penetration Testing** focuses on testing a stakeholder's internet exposure.
- **Risk and Vulnerability Assessments** combine national threat information with data collected and vulnerabilities identified through on-site assessment activities to provide tailored risk analysis reports.
- **Red Team Assessments** closely mirror an attack by an advanced adversary to test operational capabilities and maturity.
- **Validated Architecture Design Review** evaluates the resiliency of a stakeholder's systems, networks and security services.
- **Third-Party Qualification** qualifies third-party organizations to perform assessments and technical services following CISA Assessments standards, process and procedures.
- **Critical Product Evaluations** assess, within an isolated environment, the "out-of-the-box" security of products and solutions relevant to critical infrastructure operations and national resilience.
- **Cyber Resilience Review** identifies and evaluates cyber security management capabilities, maturity, and capacity to manage cyber risk during normal operations and times of operational stress.
- **External Dependency Management** assesses the activities and practices utilized by an organization to manage risks arising from external dependencies.
- **Cyber Infrastructure Survey** identifies cybersecurity controls and protective measures in place and provides an interactive dashboard for comparative analysis and valuation.



ABOUT

Our Team

The CISA Assessments team is a group of highly trained information security experts. Our mission is to measurably reduce cybersecurity risks to our Nation.

CISA leads the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure.

Our Services provide:

- **A proactive, risk-based approach** to analyzing stakeholder systems
- **Expertise** in identification of vulnerabilities, risk evaluation, and prioritized mitigation guidance
- **Comprehensive services that empower stakeholders** to increase speed and effectiveness of their cyber response capabilities.

Additional Information

CISA assessments' security services are available at no cost. Stakeholders include Federal, State, Local, Tribal and Territorial governments, as well as Critical Infrastructure private sector companies. CISA does not share attributable information without written and agreed consent from the stakeholder. CISA uses anonymized data to develop non-attributed reports for trending and analysis purposes.



GET STARTED

Capabilities and service delivery timelines are available upon request. Service availability is limited. Contact us at NCATS_INFO@hq.dhs.gov to get started. Service delivery queues are prioritized on a continuous basis to ensure no stakeholder or sector receives a disproportionate amount of resources and that the data collected is a diverse representation of the nation.



MISSION AND VISION

Mission: *Providing cybersecurity assessments to facilitate the identification of risk for the purpose of protecting the Nation's cyber infrastructure.*

Vision: *To be the preeminent government leader providing comprehensive, innovative, and dynamic cybersecurity assessments for the purpose of facilitating and protecting the federal, state, private sector and critical infrastructure networks of the United States, reducing attack surfaces, eliminating threats, and fostering partnerships across the government landscape.*

CYBER HYGIENE: VULNERABILITY SCANNING

The CISA Assessments team supports Federal, State, Local, Tribal and Territorial Governments and Critical Infrastructure partners by providing proactive testing and assessment services.

CISA's Cyber Hygiene Vulnerability Scanning is "internet scanning-as-a-service." This service continuously assesses the "health" of your internet-accessible assets by checking for known vulnerabilities and weak configurations, and recommends ways to enhance security through modern web and email standards.



SCANNING OBJECTIVES

- Maintain enterprise awareness of your internet-accessible systems
- Provide insight into how systems and infrastructure appear to potential attackers
- Drive proactive mitigation of vulnerabilities and reduce risk



SCANNING PHASES AND STAGES

PHASES

- **Target Discovery:** Identify all active internet-accessible assets (networks, systems, and hosts) to be scanned
- **Vulnerability Scanning:** Initiate non-intrusive checks to identify potential vulnerabilities and configuration weaknesses

STAGES

Pre-Planning

- Request service
- Receive Cyber Hygiene brief
- Provide target list (scope)
- Sign and return documents
- 12 hours for "critical"
- 24 hours for "high"
- 4 days for "medium"
- 6 days for "low"
- 7 days for "no vulnerabilities"

Planning

- Confirm scanning schedule
- Pre-scan notification

Execution

- Initial scan of submitted scope
- Rescan scope based on detected vulnerability severity:

Reporting

- Ongoing weekly summary report
- Vulnerability mitigation recommendations
- Detailed findings in consumable format



ABOUT

Our Team

The CISA Assessments team is a group of highly trained information security experts. Our mission is to measurably reduce cybersecurity risks to our Nation.

CISA leads the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure.

Our services provide:

- **A proactive, risk-based approach** to analyzing stakeholder systems
- **Expertise** in identification of vulnerabilities, risk evaluation, and prioritized mitigation guidance
- **Comprehensive services that empower stakeholders** to increase speed and effectiveness of their cyber response capabilities

Additional Information

CISA assessments' security services are available at no cost. Stakeholders include Federal, State, Local, Tribal and Territorial governments, as well as Critical Infrastructure private sector companies. CISA does not share attributable information without written and agreed consent from the stakeholder. CISA uses anonymized data to develop non-attributed reports for trending and analysis purposes.



GET STARTED

Capabilities and service delivery timelines are available upon request. Service availability is limited. Contact us at **NCATS_INFO@hq.dhs.gov** to get started. Service delivery queues are prioritized on a continuous basis to ensure no stakeholder or sector receives a disproportionate amount of resources and that the data collected is a diverse representation of the nation.



MISSION AND VISION

Mission: *Providing cybersecurity assessments to facilitate the identification of risk for the purpose of protecting the Nation's cyber infrastructure.*

Vision: *To be the preeminent government leader providing comprehensive, innovative, and dynamic cybersecurity assessments for the purpose of facilitating and protecting the federal, state, private sector and critical infrastructure networks of the United States, reducing attack surfaces, eliminating threats, and fostering partnerships across the government landscape.*

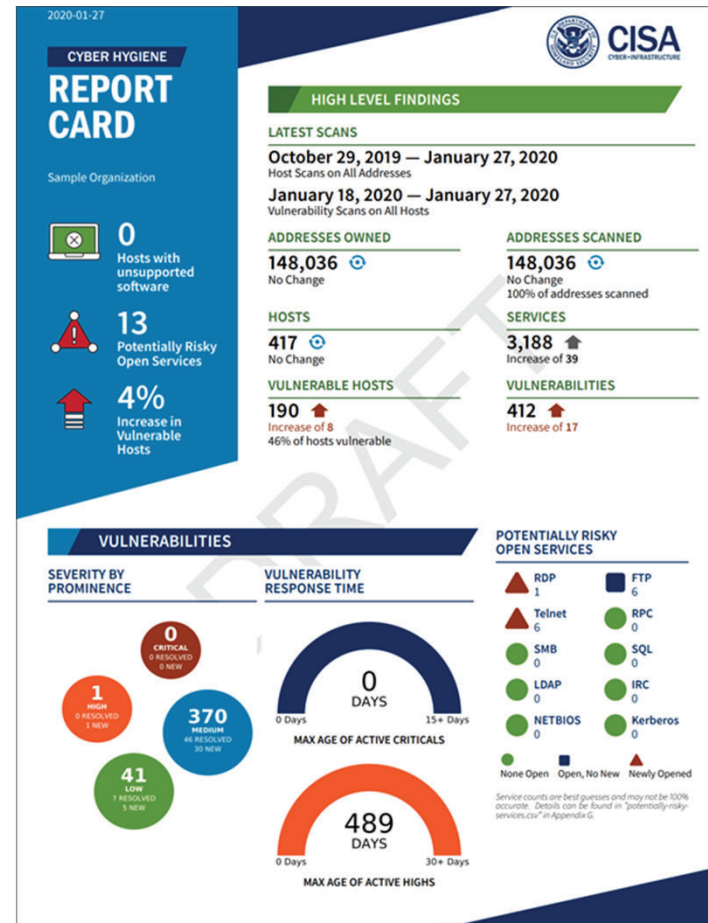
Report Card

High Level Findings

- Latest Scans
- Addresses Owned
- Addresses Scanned
- Hosts
- Services
- Vulnerable Hosts
- Vulnerabilities

Vulnerabilities

- Severity by Prominence
- Vulnerability Response Time
- Potentially Risky Open Services



HIGH VALUE ASSET ASSESSMENT

The CISA Assessments team supports Federal, State, Local, Tribal and Territorial Governments and Critical Infrastructure partners by providing proactive testing and assessment services.

CISA Assessments' High Value Asset (HVA) Assessment is similar to a Risk and Vulnerability Assessment in knowledge, skills, tools, tactics, and methodology. However, an HVA entails specific, predefined attack scenarios used consistently across the assessment targeted at critical assets selected by the Office of Management and Budget.



OBJECTIVES

- Identify weaknesses through scenario-based network penetration testing, web application testing, and social engineering
- Test stakeholder networks using real world capabilities and methodologies
- Understand how systems and infrastructure appear to potential attackers
- Coordinate with CISA Hunt and Incident Response Team to provide follow-on services within the pertinent domain



ASSESSMENT SCENARIOS AND TIMELINES

SCENARIOS

- **External Access:** Determine if HVA is accessible from the internet by an unauthorized user.
- **Phishing Campaign Assessments** measure propensity to click on email phishing lures to increase training and awareness.
- **Web Application Assessment:** Identify any exploits in web applications.
- **Internal Access:** Determine if HVA system is accessible from the internal domain by an unauthorized user.
- **Internal Threat Emulation:** Examine access level of legitimate user on HVA system and associated data.
- **Data Exfiltration:** Test ability to transfer sensitive data to external site on the internet.

TIMELINES

Pre-Planning

- Receive selection for assessment
- Receive HVA brief
- Sign and return documents

Planning

- Confirm schedule
- Establish trusted points of contact

Execution

- Perform scenario activity
- On-site testing performed as required

Post-Execution

- On-site briefing and initial recommendations
- Final report review and receipt



ABOUT

Our Team

The CISA Assessments team is a group of highly trained information security experts. Our mission is to measurably reduce cybersecurity risks to our Nation.

CISA leads the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure.

Our services provide:

- **A proactive, risk-based approach** to analyzing stakeholder systems
- **Expertise** in identification of vulnerabilities, risk evaluation, and prioritized mitigation guidance
- **Comprehensive services that empower stakeholders** to increase speed and effectiveness of their cyber response capabilities

Additional Information

CISA assessments' security services are available at no cost. Stakeholders include Federal, State, Local, Tribal and Territorial governments, as well as Critical Infrastructure private sector companies. CISA does not share attributable information without written and agreed consent from the stakeholder. CISA uses anonymized data to develop non-attributed reports for trending and analysis purposes.



GET STARTED

Capabilities and service delivery timelines are available upon request. Service availability is limited. Contact us at NCATS_INFO@hq.dhs.gov to get started. Service delivery queues are prioritized on a continuous basis to ensure no stakeholder or sector receives a disproportionate amount of resources and that the data collected is a diverse representation of the nation.



MISSION AND VISION

Mission: *Providing cybersecurity assessments to facilitate the identification of risk for the purpose of protecting the Nation's cyber infrastructure.*

Vision: *To be the preeminent government leader providing comprehensive, innovative, and dynamic cybersecurity assessments for the purpose of facilitating and protecting the federal, state, private sector and critical infrastructure networks of the United States, reducing attack surfaces, eliminating threats, and fostering partnerships across the government landscape.*

CYBER HYGIENE: WEB APPLICATION SCANNING (WAS)

The CISA Assessments team supports Federal, State, Local, Tribal and Territorial Governments and Critical Infrastructure partners by providing proactive testing and assessment services.

CISA's Cyber Hygiene Web Application Scanning is "internet scanning-as-a-service." This service assesses the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, we can recommend ways to enhance security in accordance with industry and government best practices and standards.



SCANNING OBJECTIVES

- Maintain enterprise awareness of your publicly accessible web-based assets
- Provide insight into how systems and infrastructure appear to potential attackers
- Drive proactive mitigation of vulnerabilities to help reduce overall risk

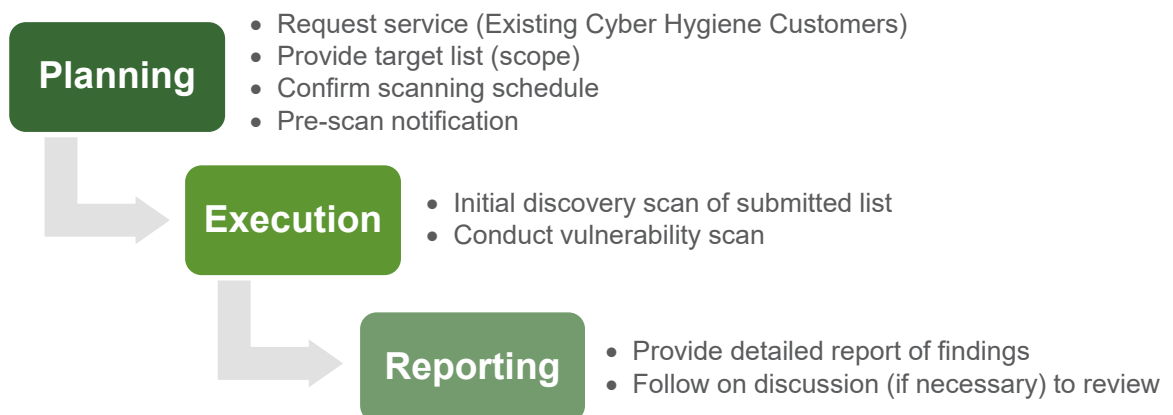


SCANNING PHASES AND OVERALL PROCESS

Scanning Phases

- **Discovery Scanning:** Identify active, internet-facing web applications
- **Vulnerability Scanning:** Initiate non-intrusive checks to identify potential vulnerabilities and configuration weaknesses

Overall Process





ABOUT

Our Team

The CISA Assessments team is a group of highly trained information security experts. Our mission is to measurably reduce cybersecurity risks to Federal Government, SLTT and critical infrastructure networks.

CISA leads the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure.

Our services provide:

- **A proactive, risk-based approach** to analyzing stakeholder systems
- **Expertise** in identification of vulnerabilities, risk evaluation, and prioritized mitigation guidance
- **Comprehensive services that empower stakeholders** to increase speed and effectiveness of their cyber response capabilities

Additional Information

CISA assessments' security services are available at no cost. Stakeholders include Federal, State, Local, Tribal and Territorial governments, as well as Critical Infrastructure private sector companies. CISA does not share attributable information without written and agreed consent from the stakeholder. CISA uses anonymized data to develop non-attributed reports for trending and analysis purposes.



GET STARTED

Capabilities and service delivery timelines are available upon request. Service availability is currently limited to existing CISA customers. Contact us at NCATS_INFO@hq.dhs.gov to get started. Service delivery queues are prioritized on a continuous basis to ensure no stakeholder or sector receives a disproportionate amount of resources and that the data collected is a diverse representation of the nation.



MISSION AND VISION

Mission: *Providing cybersecurity assessments to facilitate the identification of risk for the purpose of protecting the Nation's cyber infrastructure.*

Vision: *To be the preeminent government leader providing comprehensive, innovative, and dynamic cybersecurity assessments for the purpose of facilitating and protecting the federal, state, private sector and critical infrastructure networks of the United States, reducing attack surfaces, eliminating threats, and fostering partnerships across the government landscape.*

PHISHING CAMPAIGN ASSESSMENT

The CISA Assessments team supports Federal, State, Local, Tribal and Territorial Governments and Critical Infrastructure partners by providing proactive testing and assessment services.

CISA Assessments' Phishing Campaign Assessment (PCA) measures an organization's propensity to click on email phishing lures, commonly used to collect sensitive information or as initial access to a network. Based on CISA Assessments' testing, email phishing is the number one means of initial access into a private network. PCA results can be used to provide guidance for anti-phishing training and awareness.



CAPABILITIES

Test: Assess the behavioral responses of a specified target user base when presented with expertly crafted phishing emails emulating real world threats.

Inform: Provide leadership information on potential training and awareness improvements based on the metrics gathered through the course of the assessment.



ASSESSMENT OBJECTIVES

- Reduce risk to malicious phishing email attempts by testing and informing users
- Understand how users are enticed to click on links and report suspicious activity
- Properly emulate malicious phishing activity to provide a quality learning experience



ASSESSMENT TIMELINE

Pre-Planning

- Request assessment
- Receive PCA briefing documents
- Sign and return forms

Planning

- Confirm schedule
- Approve email templates
- Test email delivery/receipt

Execution (Six weeks)

- Receive increasingly deceptive phishing emails from pre-approved templates

Post-Execution

- Receive weekly click-rate summaries
- Final report review and receipt
- Optional retest available



ABOUT

Our Team

The CISA Assessments team is a group of highly trained information security experts. Our mission is to measurably reduce cybersecurity risks to our Nation.

CISA leads the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure.

Our services provide:

- **A proactive, risk-based approach** to analyzing stakeholder systems
- **Expertise** in identification of vulnerabilities, risk evaluation, and prioritized mitigation guidance
- **Comprehensive services that empower stakeholders** to increase speed and effectiveness of their cyber response capabilities.

Additional Information

CISA assessments' security services are available at no cost. Stakeholders include Federal, State, Local, Tribal and Territorial governments, as well as Critical Infrastructure private sector companies. CISA does not share attributable information without written and agreed consent from the stakeholder. CISA uses anonymized data to develop non-attributed reports for trending and analysis purposes.



GET STARTED

Capabilities and service delivery timelines are available upon request. Service availability is limited. Contact us at NCATS_INFO@hq.dhs.gov to get started. Service delivery queues are prioritized on a continuous basis to ensure no stakeholder or sector receives a disproportionate amount of resources and that the data collected is a diverse representation of the nation.



MISSION AND VISION

Mission: *Providing cybersecurity assessments to facilitate the identification of risk for the purpose of protecting the Nation's cyber infrastructure.*

Vision: *To be the preeminent government leader providing comprehensive, innovative, and dynamic cybersecurity assessments for the purpose of facilitating and protecting the federal, state, private sector and critical infrastructure networks of the United States, reducing attack surfaces, eliminating threats, and fostering partnerships across the government landscape.*

VALIDATED ARCHITECTURE DESIGN REVIEW

The CISA Assessments team supports Federal, State, Local, Tribal and Territorial Governments and Critical Infrastructure partners by providing proactive testing and assessment services.

CISA Assessments' Validated Architecture Design Review (VADR) is an assessment based on federal and industry standards, guidelines, and best practices. Assessments can be conducted on Information Technology (IT) or Operational Technology (OT) infrastructures.



CAPABILITIES

Architecture Design Review: In-depth review of network architecture design and interconnectivity to internal and external systems focused on defensive strategies.

System Configuration and Log Review: Detailed review of system settings and activity to determine the susceptibility to potential attacks and baseline normal behavior to find anomalies.

Network Traffic Analysis: Utilizes a combination of open-source and commercial tools to identify anomalous communications, which could indicate suspicious activity or misconfiguration.



ASSESSMENT OBJECTIVES

- Reduce risk to the Nation's critical infrastructure components.
- Analyze systems based on standards, guidelines, and best practices.
- Ensure effective defense-in-depth strategies.
- Provide findings and practical mitigations for improving operational maturity and enhancing cybersecurity posture.



ASSESSMENT TIMELINE

Pre-Planning

- Request VADR
- Sign and return documents
- Schedule Execution Activities
- Confirm Schedule

Execution

- Review submitted architecture
- Analyze packet captures

Planning

- Submit VADR specific documents and network diagram
- Schedule assessment planning meeting
- Submit network configurations, logs, and packet captures
- Interviews with key personnel

Post-Execution

- Out-brief – provides initial findings
- Final report (approximately 4 weeks)
- Follow-up on remediation actions – 180 days

ABOUT

Our Team

The CISA Assessments team is a group of highly trained information security experts. Our mission is to measurably reduce cybersecurity risks to our Nation.

CISA leads the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure.

Our services provide:

- **A proactive, risk-based approach** to analyzing stakeholder systems
- **Expertise** in identification of vulnerabilities, risk evaluation, and prioritized mitigation guidance
- **Comprehensive services that empower stakeholders** to increase speed and effectiveness of their cyber response capabilities.

Additional Information

CISA assessments' security services are available at no cost. Stakeholders include Federal, State, Local, Tribal and Territorial governments, as well as Critical Infrastructure private sector companies. CISA does not share attributable information without written and agreed consent from the stakeholder. CISA uses anonymized data to develop non-attributed reports for trending and analysis purposes.

GET STARTED

Capabilities and service delivery timelines are available upon request. Service availability is limited. Contact us at NCATS_INFO@hq.dhs.gov to get started. Service delivery queues are prioritized on a continuous basis to ensure no stakeholder or sector receives a disproportionate amount of resources and that the data collected is a diverse representation of the nation.

MISSION AND VISION

Mission: *Providing cybersecurity assessments to facilitate the identification of risk for the purpose of protecting the Nation's cyber infrastructure.*

Vision: *To be the preeminent government leader providing comprehensive, innovative, and dynamic cybersecurity assessments for the purpose of facilitating and protecting the federal, state, private sector and critical infrastructure networks of the United States, reducing attack surfaces, eliminating threats, and fostering partnerships across the government landscape.*

RISK AND VULNERABILITY ASSESSMENT

The CISA Assessments team supports Federal, State, Local, Tribal and Territorial Governments and Critical Infrastructure partners by providing proactive testing and assessment services.

CISA Assessments' Risk and Vulnerability Assessment (RVA) is a one-on-one engagement with stakeholders that combines open-source national threat and vulnerability information with data collected through remote and onsite assessment activities to provide actionable risk analysis reports with remediation recommendations prioritized by severity and risk.



CAPABILITIES

Penetration Testing: CISA Assessments conducts an array of tests to determine susceptibility to an actual real-world attack by infiltrating the target environment using current tactics, techniques, and procedures. Specific types of testing and assessments include network, web application, wireless, war dial, and social engineering in the form of an email phishing campaign.

Configuration Review: CISA Assessments reviews and analyzes operating system and database settings and configurations, which the team compares to industry standards, guidelines, and best practices to identify security issues.



ASSESSMENT OBJECTIVES

- Identify weaknesses through network, system, and application penetration testing
- Test stakeholders using a standard, repeatable methodology to deliver actionable findings and recommendations
- Analyze collected data to identify security trends across all RVA stakeholder environments



ASSESSMENT TIMELINE

Pre-Planning

- Request RVA
- Receive RVA brief
- Sign and return documents

Planning

- Confirm schedule
- Establish Trusted Point of Contact
- Determine RVA services, scope, and logistics during pre-assessment call(s)

Execution (Ten Days)

- One week external testing
- One week internal testing
- Remote Penetration Testing – external only

Post-Execution

- Out-Brief – provide initial findings
- Report review and receipt – 10 days
- Follow-up on remediation actions – 180 day



ABOUT

Our Team

The CISA Assessments team is a group of highly trained information security experts. Our mission is to measurably reduce cybersecurity risks to our Nation.

CISA leads the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure.

Our services provide:

- **A proactive, risk-based approach** to analyzing stakeholder systems
- **Expertise** in identification of vulnerabilities, risk evaluation, and prioritized mitigation guidance
- **Comprehensive services that empower stakeholders** to increase speed and effectiveness of their cyber response capabilities

Additional Information

CISA assessments' security services are available at no cost. Stakeholders include Federal, State, Local, Tribal and Territorial governments, as well as Critical Infrastructure private sector companies. CISA does not share attributable information without written and agreed consent from the stakeholder. CISA uses anonymized data to develop non-attributed reports for trending and analysis purposes.



GET STARTED

Capabilities and service delivery timelines are available upon request. Service availability is limited. Contact us at NCATS_INFO@hq.dhs.gov to get started. Service delivery queues are prioritized on a continuous basis to ensure no stakeholder or sector receives a disproportionate amount of resources and that the data collected is a diverse representation of the nation.



MISSION AND VISION

Mission: *Providing cybersecurity assessments to facilitate the identification of risk for the purpose of protecting the Nation's cyber infrastructure.*

Vision: *To be the preeminent government leader providing comprehensive, innovative, and dynamic cybersecurity assessments for the purpose of facilitating and protecting the federal, state, private sector and critical infrastructure networks of the United States, reducing attack surfaces, eliminating threats, and fostering partnerships across the government landscape.*

REMOTE PENETRATION TESTING

The CISA Assessments team supports Federal, State, Local, Tribal and Territorial Governments and Critical Infrastructure partners by providing proactive testing and assessment services.

CISA Assessments' Remote Penetration Test (RPT) utilizes a dedicated remote team to assess and identify vulnerabilities and work with customers to eliminate exploitable pathways. RPTs are similar to risk and vulnerability assessments but focus only on externally accessible systems with a tradeoff made for more service capacity at the expense of assessment scope. As a remote service, it is less costly and more scalable than on-site offerings; however, it is more limited in organizational insight and context.



SCENARIOS

External Penetration Test: Verifying if the stakeholder network is accessible from the public domain by an unauthorized user by assessing open ports, protocols, and services.

External Web Application Test: Evaluating web applications for potential exploitable vulnerabilities; the test can include automated scanning, manual testing, or a combination of both methods.

Phishing Assessment: Testing through carefully crafted phishing emails containing a variety of malicious payloads to the trusted point of contact.



ASSESSMENT OBJECTIVES

- Conduct assessments to identify vulnerabilities and work with customers to eliminate exploitable pathways.
- Simulate the tactics and techniques of real-world threats and malicious adversaries.
- Test centralized data repositories and externally accessible assets/resources.
- Avoid causing disruption to the customer's mission, operation, and network infrastructure.



ASSESSMENT TIMELINE

Pre-Planning

- Request RPT
- Receive RPT Capabilities Brief
- Sign and return RPT Rules of Engagement

Planning

- Confirm schedule
- Establish trusted points of contact

- Determine RPT services, scope, and logistics during pre-assessment call(s)

Execution (Up to Six Weeks)

- Dependent on resource availability
- Critical findings are immediately disclosed

Reporting

- Briefing and initial recommendations
- Final report review and receipt – 10 days
- Follow-up on mitigation actions – 180 day

ABOUT

Our Team

The CISA Assessments team is a group of highly trained information security experts. Our mission is to measurably reduce cybersecurity risks to our Nation.

CISA leads the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure.

Our services provide:

- **A proactive, risk-based approach** to analyzing stakeholder systems
- **Expertise** in identification of vulnerabilities, risk evaluation, and prioritized mitigation guidance
- **Comprehensive services that empower stakeholders** to increase speed and effectiveness of their cyber response capabilities

Additional Information

CISA assessments' security services are available at no cost. Stakeholders include Federal, State, Local, Tribal and Territorial governments, as well as Critical Infrastructure private sector companies. CISA does not share attributable information without written and agreed consent from the stakeholder. CISA uses anonymized data to develop non-attributed reports for trending and analysis purposes.

GET STARTED

Capabilities and service delivery timelines are available upon request. Service availability is limited. Contact us at NCATS_INFO@hq.dhs.gov to get started. Service delivery queues are prioritized on a continuous basis to ensure no stakeholder or sector receives a disproportionate amount of resources and that the data collected is a diverse representation of the nation.

MISSION AND VISION

Mission: *Providing cybersecurity assessments to facilitate the identification of risk for the purpose of protecting the Nation's cyber infrastructure.*

Vision: *To be the preeminent government leader providing comprehensive, innovative, and dynamic cybersecurity assessments for the purpose of facilitating and protecting the federal, state, private sector and critical infrastructure networks of the United States, reducing attack surfaces, eliminating threats, and fostering partnerships across the government landscape.*

RED TEAM ASSESSMENT

The CISA Assessments team supports Federal, State, Local, Tribal and Territorial Governments and Critical Infrastructure partners by providing proactive testing and assessment services.

CISA Assessments' Red Team Assessment (RTA) is a comprehensive evaluation of an information technology (IT) environment. Simulation of advanced persistent threats (APTs) can assist stakeholders in determining their security posture by testing the effectiveness of response capabilities to a determined adversarial presence. RTAs are crafted specifically to test the people, processes, and technologies defending a network.



ASSESSMENT PHASES

Threat Simulation: CISA Assessments simulate APT tactics, techniques, and procedures using publicly available tools and data to access, navigate, and persist in a stakeholder's environment.

Measureable Events: Once entrenched in the network, a series of events are initiated, specifically intended to provoke a security response. Measured effectiveness of the people, processes, and technologies defending a stakeholder's network is determined by observable response-driven metrics.



ASSESSMENT OBJECTIVES

- Evaluate people, processes, and technologies responsible for defending the stakeholder's network.
- Provide stakeholder executives actionable insight to their cybersecurity posture and practical training for technical personnel.



ASSESSMENT TIMELINE

Pre-Planning

- Request assessment
- Receive RTA brief
- Sign and return documents

Planning

- Confirm schedule
- Define scope
- Establish trusted points of contact

Execution (90 Days)

- Open-source intelligence
- Simulate APT
- Security response testing through activation of measurable Events

Post-Execution

- On-site out-brief and training



ABOUT

Our Team

The CISA Assessments team is a group of highly trained information security experts. Our mission is to measurably reduce cybersecurity risks to our Nation.

CISA leads the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure.

Our services provide:

- **A proactive, risk-based approach** to analyzing stakeholder systems
- **Expertise** in identification of vulnerabilities, risk evaluation, and prioritized mitigation guidance
- **Comprehensive services that empower stakeholders** to increase speed and effectiveness of their cyber response capabilities.

Additional Information

CISA assessments' security services are available at no cost. Stakeholders include Federal, State, Local, Tribal and Territorial governments, as well as Critical Infrastructure private sector companies. CISA does not share attributable information without written and agreed consent from the stakeholder. CISA uses anonymized data to develop non-attributed reports for trending and analysis purposes.



GET STARTED

Capabilities and service delivery timelines are available upon request. Service availability is limited. Contact us at NCATS_INFO@hq.dhs.gov to get started. Service delivery queues are prioritized on a continuous basis to ensure no stakeholder or sector receives a disproportionate amount of resources and that the data collected is a diverse representation of the nation.



MISSION AND VISION

Mission: *Providing cybersecurity assessments to facilitate the identification of risk for the purpose of protecting the Nation's cyber infrastructure.*

Vision: *To be the preeminent government leader providing comprehensive, innovative, and dynamic cybersecurity assessments for the purpose of facilitating and protecting the federal, state, private sector and critical infrastructure networks of the United States, reducing attack surfaces, eliminating threats, and fostering partnerships across the government landscape.*

CRITICAL PRODUCT EVALUATION

The CISA Assessments team supports Federal, State, Local, Tribal and Territorial Governments and Critical Infrastructure partners by providing proactive testing and assessment services.

CISA Assessments' Critical Product Evaluation (CPE) is a multi-week, comprehensive evaluation of a vendor's solution or appliance that ubiquitously supports critical infrastructure operations or other national endeavors to improve the "out of the box" and recommended security implementation of the product, ultimately improving our national resiliency.



ASSESSMENT OBJECTIVES

- Enumerate the vulnerabilities associated with the product's in-scope software, firmware, hardware
- Attempt exploitation of vulnerabilities that present the greatest risk using known exploits, or, if practical, develop new code or technique
- Capture indicators-of-compromise information to help incident responders determine the existence or extent of an incident
- Capture assessment methods
- Assist in developing remediation or mitigation strategies.



ASSESSMENT PHASES AND TIMELINE

Pre-Planning

- Request assessment
- Receive CPE brief
- Sign and return documents

Planning

- Define scope and confirm schedule
- Coordinate delivery of the system(s)-under-test (SUT)

Execution (Tailored*)

- Check-in and Configuration: setup and configure for normal operation

- Enumeration: list software and hardware interfaces
- Deconstructive Testing: mapping the attack surface and developing threat scenarios
- Target Analysis: execute attack vector testing and attempt exploitation

Post-Execution

- Coordinate SUT return**
- Report generation
- Out-brief with evaluation team

* Length of time for a CPE is based on the complexity of the SUT. Generally, eight-weeks is the starting point, however, this time can be amended during the scoping meetings or during the course of the evaluation.

** Equipment may become damaged during the course of testing.



ABOUT CISA ASSESSMENTS

Our Team

The CISA Assessments team is a group of highly trained information security experts. Our mission is to measurably reduce cybersecurity risks to our Nation.

CISA leads the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure.

Our services provide:

- **A proactive, risk-based approach** to analyzing stakeholder systems
- **Expertise** in identification of vulnerabilities, risk evaluation, and prioritized mitigation guidance
- **Comprehensive services that empower stakeholders** to increase speed and effectiveness of their cyber response capabilities.

Additional Information

CISA assessments' security services are available at no cost. Stakeholders include Federal, State, Local, Tribal and Territorial governments, as well as Critical Infrastructure private sector companies. CISA does not share attributable information without written and agreed consent from the stakeholder. CISA uses anonymized data to develop non-attributed reports for trending and analysis purposes.



GET STARTED

Capabilities and service delivery timelines are available upon request. Service availability is limited. Contact us at NCATS_INFO@hq.dhs.gov to get started. Service delivery queues are prioritized on a continuous basis to ensure no stakeholder or sector receives a disproportionate amount of resources and that the data collected is a diverse representation of the nation.



MISSION AND VISION

Mission: *Providing cybersecurity assessments to facilitate the identification of risk for the purpose of protecting the Nation's cyber infrastructure.*

Vision: *To be the preeminent government leader providing comprehensive, innovative, and dynamic cybersecurity assessments for the purpose of facilitating and protecting the federal, state, private sector and critical infrastructure networks of the United States, reducing attack surfaces, eliminating threats, and fostering partnerships across the government landscape.*



Hunt and Incident Response Team (HIRT)

THE NATIONAL CYBERSECURITY & COMMUNICATIONS INTEGRATION CENTER (NCCIC) OPERATES AT THE INTERSECTION OF THE PRIVATE SECTOR, CIVILIAN, LAW ENFORCEMENT, INTELLIGENCE, AND DEFENSE COMMUNITIES, APPLYING UNIQUE ANALYTIC PERSPECTIVES, ENSURING SHARED SITUATIONAL AWARENESS, AND ORCHESTRATING SYNCHRONIZED RESPONSE EFFORTS WHILE PROTECTING THE CONSTITUTIONAL AND PRIVACY RIGHTS OF AMERICANS IN BOTH THE CYBERSECURITY AND COMMUNICATIONS DOMAINS.

The NCCIC HIRT provides expert intrusion analysis and mitigation guidance to clients who lack in-house capability or require additional assistance with responding to a cyber incident. HIRT supports federal departments and agencies, state and local governments, the private sector (industry and critical infrastructure asset owners and operators), academia, and international organizations.

NCCIC HIRT performs both on-site and remote cybersecurity incident response. A typical engagement includes log, network traffic, and host analysis. The goal is to discover malicious actors, acquire, and analyze the malicious tools, and provide mitigation guidance.

NCCIC HIRT is uniquely positioned with knowledge of both unclassified and classified actor tactics, techniques, and procedures compiled from public and private sector partners. HIRT works closely with law enforcement, the intelligence community, and international partners to provide a coordinated and comprehensive response. The NCCIC HIRT provides on-site support for numerous large-scale engagements each year, covering a wide variety of organizations.

HUNT

The goal of a hunt is to use tools and techniques to proactively check for and mitigate against malicious actor activity. More specifically, it will be charged to search for exploitation tools, tactics, procedures and their associated artifacts. Performed from within the customer environment on internal networks and hosts, it will encompass any systems that were identified by a Risk Review. Hunts are scoped to those systems that are part of a risk vetting process. The initial hunt will be targeted and precise, but results of an initial analysis may warrant the expansion of its scope to include additional systems, segments

or environments. Ultimately, the analysis will further measure potential risks to the integrity, confidentiality, and availability of systems that need immediate attention. If evidence of a potential compromise is recognized, the Incident Response Team (IRT) will review agency materials and conduct interviews with technical staff, management, and senior leadership to further understand possible security gaps, thus allowing for more effective mitigation. As part of this mitigation response, a document incorporating actionable guidance will be provided.

INCIDENT RESPONSE

If evidence of a potential compromise is recognized, the Incident Response Team (IRT) will review agency materials and conduct interviews with technical staff, management, and senior leadership to further understand possible security

gaps, thus allowing for more effective mitigation. As part of this mitigation response, a document incorporating actionable guidance will be provided.

TOOLS, TECHNIQUES, AND ARTIFACTS

A hunt and incident response will utilize tools, techniques, and artifacts to determine where a system has been compromised. They are listed as follows:












- Existing documentation to include policies, procedures and processes
- Existing customer documentation
- Network traffic analysis
- System owner interviews
- Host-based analysis
- Network infrastructure analysis
- Review of existing customer logs
- Data mappings and other diagrams

ADVANTAGES

- HIRT improves in-house lab capabilities and onsite processes
- HIRT leverages total HIRT, US-CERT, ICS-CERT, and NCCIC capabilities to assist the client
- HIRT utilizes defined, repeatable processes
- HIRT is able to create customized mitigation plan for the client

SERVICE OFFERINGS

The HIRT works onsite and remotely to provide services to eligible clients. All of the following are offered on a voluntary basis:

	Incident Triage: Process taken to scope the severity of an incident and determine required resources for action		Security Program Review: A review of the client's existing security roles, responsibilities, and policies to identify possible organizational or information-sharing gaps
	Network Topology Review: Assessment of network ingress, egress, remote access, segmentation, and interconnectivity, with resulting recommendations for security enhancements		Malware Analysis: Reverse engineering of malware artifacts to determine functionality and build indicators
	Infrastructure Configuration Review: Analysis of core devices on the network which are or can be used for network security (e.g., prevention, monitoring, or enforcement functions)		Mitigation: Actionable guidance to improve the organization's security posture, including incident-specific recommendations, security best practices, and recommended tactical measures
	Log Analysis: Examination of logs from network and security devices to illuminate possible malicious activity		Digital Media Analysis: Technical forensic examination of digital artifacts to detect malicious activity and develop further indicators
	Incident Specific Risk Overview: Materials and in-person briefings for technical, program manager, or senior leadership audience; cover current cyber risk landscape, including classified briefings to cleared staff when appropriate		Control Systems Incident Analysis: Analysis of supervisory control and data acquisition devices, process control, distributed control, and any other systems that control, monitor, and manage critical infrastructure
	Hunt Analysis: Deployment of network hunting tools to proactively detect indicators of compromise (IOC)		

SEND REPORTS TO NCCIC

HIRT encourages reports of cybersecurity incidents, possible malicious code, vulnerabilities, and phishing attacks. Submit a report via phone: 1-888-282-0870 or email: NCCICCustomerService@hq.dhs.gov.



CISA
CYBER+INFRASTRUCTURE

DEFEND TODAY. SECURE TOMORROW.

CYBERSECURITY ASSESSMENTS SUMMARY

Name	Validated Architecture Design Review (VADR)	Phishing Campaign Assessment (PCA)	Vulnerability Scanning (Formally Cyber Hygiene)	Remote Penetration Test (RPT)	Network Risk and Vulnerability Assessment (RVA)
Purpose	Provide analysis and representation of asset owner's network traffic, data flows, and device relationships and identifies anomalous communications flows.	Measure the susceptibility of an organization's personnel to social engineering attacks, specifically email phishing attacks.	Identify public-facing Internet security risks, through service enumeration and vulnerability scanning	Perform external penetration testing and security services to identify risks and externally exploitable pathways into systems, networks and applications.	Perform penetration testing and security services to identify risks and vulnerabilities within IT systems, networks and applications
Scope	Industrial Control Systems / Network Architecture/ Network Traffic	Organization / Business Unit / Email Service	Public-Facing, Network-Based IT Service	Organization / Business Unit / Network-Based IT Service	Organization / Business Unit / Network-Based IT Service
Time to Execute	Variable (Hours to Days)	Approximately 6 Weeks	Continuous	Up to 6 weeks	Two weeks of testing
Information Sought	Network design, system configurations, log files, interdependencies, and its applications	Phishing "click rate" metrics compared to attack sophistication	Network service and vulnerability information	Network, Database, Application scope and/or access to be tested with various security tools	Network, Database, Application scope and/or access to be tested with various security tools
Preparation	Coordinated via Email. Planning calls	Formal rules of engagement and pre-planning	Signed agreement letter and IP address scope to be tested	Formal rules of engagement and extensive pre-planning	Formal rules of engagement and extensive pre-planning
Participants	Control system operators/ engineers, IT personnel, and OT personnel	IT/Security Manager, Network Administrators, end users	IT/Security Manager and Network Administrators	Management stakeholders, IT/Security Manager, Network Administrators & System Owners.	Management stakeholders, IT/Security Manager, Network Administrators, and System Owners.
Delivered By	Contact the Cybersecurity Advisor mailbox at cyberadvisor@hq.dhs.gov for more information or to request services				



Preparing for a Cyber Incident

FBI Internet Crime Complaint Center (IC3):

Report individual instances of cybercrime to the IC3, which accepts complaints from both victim and third parties.

<https://www.ic3.gov>

National Cyber Investigative Joint Task Force (NCIJTF):

24/7 CyWatch Command Center (855) 292-3937 or

cywatch@fbi.gov



Although every organization strives to never suffer from a cyber attack, the increasing use of the internet and expanding digital landscape makes it more likely that every organization will one day fall victim to a data breach, ransomware, or other cyber incident.

Preparation, which includes developing an incident response plan, is key to an effective response that minimizes harm and expedites recovery. One way to accomplish that is to establish a point of contact with your local FBI field office:

<https://www.fbi.gov/contact-us/field-offices>

Benefits of Working with the FBI:

- The FBI can respond with a range of investigative assets, all coordinated through the local FBI field office. These include Special Agents, Computer Scientists, and Intelligence Analysts in every field office who specialize in computer intrusion investigations. They also include enhanced resources like the Cyber Action Team, a rapid response team of cyber investigation experts who can deploy nearly anywhere in the world to provide advanced digital forensics and incident response capabilities to identify, collect, and analyze the most relevant and immediately actionable evidence of a computer intrusion.
- The FBI pursues investigations that can identify the source of the intrusion and provide context so you understand why you may have been targeted.
- The U.S. government can impose consequences for illicit acts, including indictment, prosecution, imposition of sanctions, and efforts to name and shame the responsible actors.

A relationship with the FBI can foster information sharing that proves beneficial both to potential victim organizations and law enforcement.

Responding to a Cyber Incident

Realities of Working with the FBI:

- ***We treat victims as victims.*** The FBI's role is to identify the responsible cyber actors and bring them to justice, not to interfere with your organization's efforts to respond, remediate, and restore operations. Whenever practicable, protective orders are sought to reduce public disclosure of sensitive information, and exemptions are claimed to guard against any investigative or other sensitive information being released.
- ***The FBI strives to minimize disruptions to your business operations.*** The FBI pursues investigative measures that avoid computer downtime, often seeking only log files and images of affected machines. The FBI also does our best to schedule witness interviews in advance, and avoid displacing employees whenever possible.
- ***The FBI seeks only technical intrusion details, not sensitive internal communications evaluating your company's security.*** The FBI works closely with incident response firms as permitted by a victim to obtain relevant information for investigative purposes. If evidence is commingled with customer data, we partner with your technical personnel to locate artifacts of the intrusion while seeking to avoid sensitive third party data. There may be times when sensitive third-party data is intermingled with information or evidence regarding the intrusion.
- ***The FBI is law enforcement, not regulators.*** As a general rule, the FBI doesn't share cyber incident information with regulators, and refer regulators to the victim itself for further information. In fact, the Federal Trade Commission and Securities & Exchange Commission have stated publicly that they view reporting favorably.



WATER AND WASTEWATER SYSTEMS

CYBERSECURITY 2021 STATE OF THE SECTOR



Water Sector Coordinating Council



JUNE 2021

CONTENTS

Executive Summary.....2

Cybersecurity Needs in the Sector5

Service and Ownership Structure7

Frequency of Risk Assessments9

Risk Management Plans Addressing Cybersecurity10

Risk Management Challenges.....10

Information-Sharing Concerns11

Cybersecurity Program Challenges.....12

IT- and OT-networked Assets13

IT and OT Management and Workforce16

Current Focus on Cybersecurity as a Priority.....18

Cybersecurity Resources Used in the Sector18

Training19

Next Steps.....21



Executive Summary

With threats from increasingly sophisticated and destructive attackers, cybersecurity has become a top priority for water and wastewater systems. Recent incidents have added urgency to discussions within the sector and with Congress and in federal agencies on how best to help utilities improve their cybersecurity.

To help guide discussions with policymakers and to inform the sector's own cybersecurity programs, the Water Sector Coordinating Council (WSCC) - an advisory body comprising the national water and wastewater associations, the sector's research foundation and WaterISAC - collaborated on a utility survey to develop a picture of current cybersecurity practices in the sector to better articulate the challenges and needs of the sector.

This voluntary survey was distributed to utilities across the country by the nation's water and wastewater associations. The results represent a first-of-its-kind snapshot of the Water and Wastewater Systems Sector cybersecurity posture.

The survey, conducted in April 2021, resulted in 606 responses from water and wastewater utilities. The results show a range of cybersecurity preparedness levels across the sector, with many excelling in their efforts with current resources but with others demonstrating room for improvement and a need for greater support.

Water Sector Coordinating Council

Member Organizations

- American Water Works Association
- Association of Metropolitan Water Agencies
- National Association of Water Companies
- National Association of Clean Water Agencies
- National Rural Water Association
- Water Environment Federation
- Water Information Sharing and Analysis Center
- The Water Research Foundation

The Water Sector Coordinating Council is a policy, strategy and coordination mechanism for the sector in interactions with the government and other sectors on critical infrastructure security and resilience issues.

Challenges

Like all sectors, water and wastewater systems are targets, directly or indirectly, of cyber attackers, but complicating any set of solutions is the demographics of the sector. There are approximately 52,000 community water systems and approximately 16,000 wastewater systems in the United States.

Among these utilities are a wide range of capabilities and capacities for cybersecurity enhancement. Many are subject to economic disadvantages typical of rural and urban communities. Others do not have access to a cybersecurity workforce. Operating in the background is that these utilities are struggling to maintain and replace infrastructure, maintain revenues while addressing issues of affordability, and comply with safe and clean water regulations.

Needs

Survey respondents identified several needs to help them improve cybersecurity.

The top four categories are:

- Training and education specific to the water sector,
- Technical assistance, assessments, and tools,
- Cybersecurity threat information, and
- Federal loans and grants.

With the exception of federal loans and grants, many such resources already exist between those developed by the sector itself and those contributed by federal agencies. But clearly there is a need for additional resources in order to reach a greater audience among our large and diverse sector. The development and promotion of these resources will require a combined effort between the sector, government agencies, and partners.

Further, nearly 30% indicated a need for information technology (IT) and operational technology (OT) supply chain integrity, which demands strong federal leadership.

Respondents by Job Type

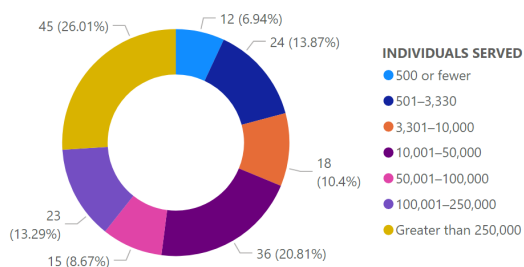
ANSWER CHOICES	RESPONSES	
CIO, CTO, CFO	9.76%	48
CISO, Sr. Security Analyst, System Administrator	7.93%	39
IT Manager, IT Specialist	14.84%	73
Other Executive Management or Board Member	28.46%	140
Water Engineer, Operations Director	39.02%	192
TOTAL		492

Cybersecurity Needs in the Sector

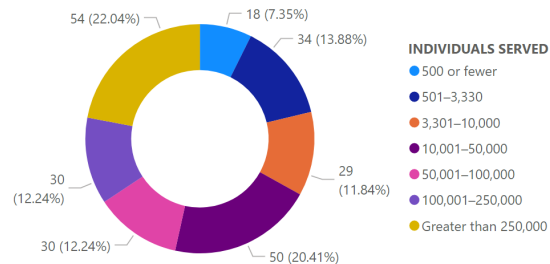
The following sector needs were identified by respondents. Further breakdown of needs by utility size are provided in the charts below.

ANSWER CHOICES	RESPONSES	
Technical assistance, advice, assessments or other support	47.47%	282
Federal grants or loans for cybersecurity equipment or services	41.08%	244
Training and education targeting the water sector	51.01%	303
Assurance of supply chain integrity for IT and OT hardware and software	29.12%	173
Funding to hire cybersecurity personnel	29.80%	177
Cybersecurity threat information	41.25%	245
I'm not sure	17.68%	105
No assistance is needed	12.46%	74
Total Respondents: 594		

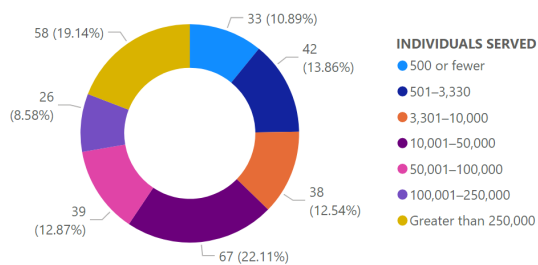
Count of NEED Assurance of supply chain integrity for IT and OT hardware and software by INDIVIDUALS SERVED



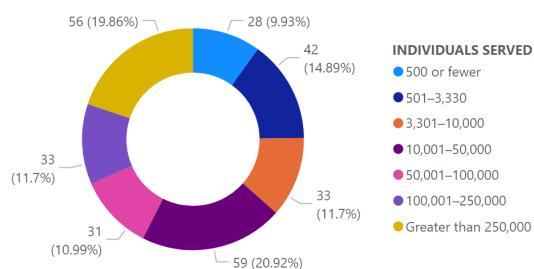
Count of NEED Cybersecurity threat information by INDIVIDUALS SERVED



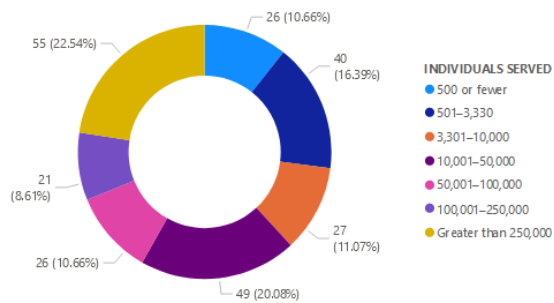
Count of NEED Training and education targeting the water sector by INDIVIDUALS SERVED



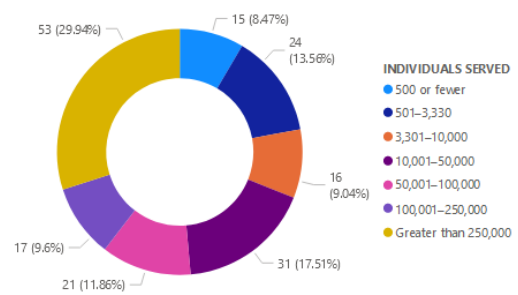
Count of NEED Technical assistance, advice, assessments or other support by INDIVIDUALS SERVED



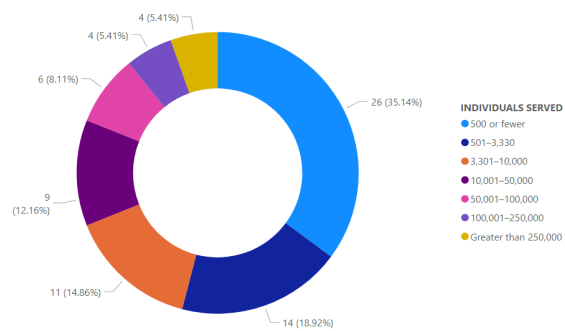
Count of NEED Federal grants or loans for cybersecurity equipment or services by INDIVIDUALS SERVED



Count of NEED Funding to hire cybersecurity personnel by INDIVIDUALS SERVED

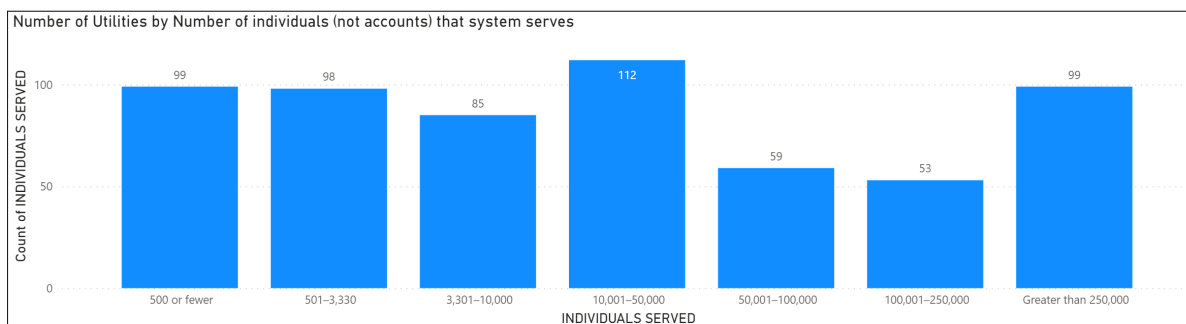


Count of NEED No assistance is needed by INDIVIDUALS SERVED



Service and Ownership Structure

PRIMARY SERVICE	Department of a municipality or county	Private non-profit/cooperative	Privately owned or investor-owned	Special district or independent government entity	Total
Combined Drinking Water and Wastewater	196	12	15	77	300
Drinking Water Only	90	43	22	87	242
Wastewater Only	25	1	2	34	62
Total	311	56	39	198	604



51.4% of survey respondents are with a department of a **municipality** or county.

32.7% of survey respondents are with a **special district** or independent government entity.

9.3% of survey respondents are with a **private non-profit/cooperative**. **6.4%** of survey respondents are with a **privately-owned or investor-owned utility**.

49.8% of survey respondents represent **combined drinking water and wastewater systems**. **40%** of survey respondents represent **drinking water-only systems**. And **10.2%** of respondents represent **wastewater-only systems**.

PERCENT UTILITY 2021 BUDGET ALLOCATION FOR IT CYBERSECURITY	500 or fewer	501–3,330	3,301– 10,000	10,001– 50,000	50,001– 100,000	100,001– 250,000	Greater than 250,000	Total
1%–5%	6	19	18	26	20	12	29	130
6%–10%	1		4	10	4	6	12	37
Don't know	17	15	20	23	14	17	28	134
Greater than 10%	1	3	4	4		3	9	24
Less than 1%	64	54	33	33	13	11	14	222
Not applicable; IT cybersecurity is managed at the municipal or county government level	6	3	5	11	7	3	4	39
Total	95	94	84	107	58	52	96	586

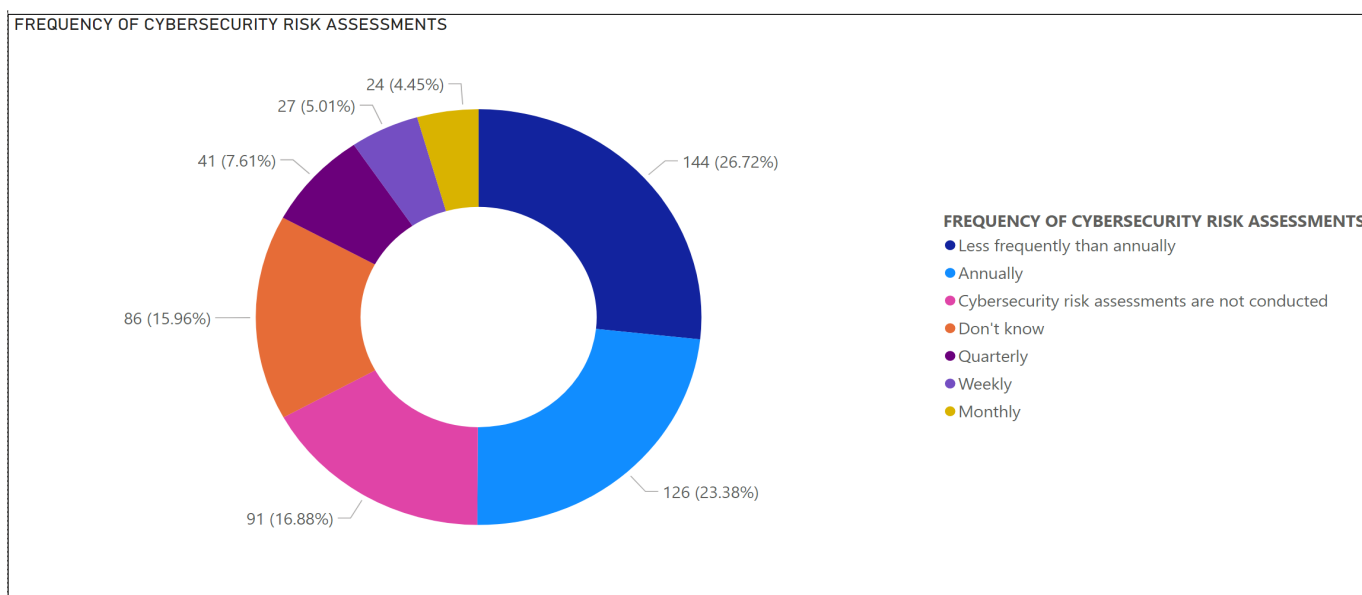
PERCENT UTILITY 2021 BUDGET ALLOCATION FOR OT CYBERSECURITY	500 or fewer	501–3,330	3,301– 10,000	10,001– 50,000	50,001– 100,000	100,001– 250,000	Greater than 250,000	Total
1%–5%	8	19	14	26	15	15	26	123
6%–10%			3	10	2	5	9	29
Don't know	19	17	21	25	12	13	30	137
Greater than 10%	1	1	3			2	3	10
Less than 1%	62	54	40	39	26	14	28	263
Not applicable; OT cybersecurity is managed at the municipal or county government level	5	3	3	8	3	3		25
Total	95	94	84	108	58	52	96	587

A representative sampling across all size systems provides the following 2021 budget allocations for cybersecurity:

- 38% of systems allocate less than 1% of budget to **IT** cybersecurity.
- 22.1% of systems allocate 1–5% of budget to **IT** cybersecurity.
- 6.3% of systems allocate 6–10% of budget to **IT** cybersecurity.
- 4.1% of systems allocate greater than 10% of budget to **IT** cybersecurity.
- 44.8% of systems allocate less than 1% of budget to **OT** cybersecurity.
- 20.95% of systems allocate 1–5% of budget to **OT** cybersecurity.
- 4.9% of systems allocate 6–10% of budget to **OT** cybersecurity.
- 1.7% of systems allocate greater than 10% of budget to **OT** cybersecurity.

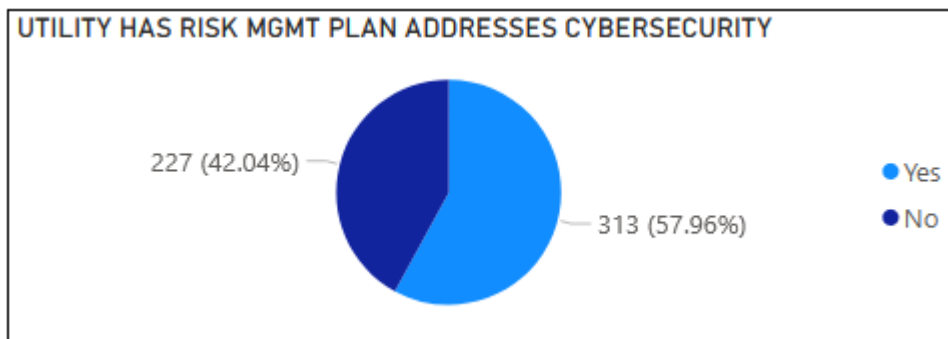
Frequency of Risk Assessments

Risk assessment is defined as the process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of a system. Risk management includes threat and vulnerability analyses as well as analyses of adverse effects on individuals arising from information processing and considers mitigations provided by security and privacy controls planned or in place. Synonymous with risk analysis. [NIST SP 800-53r5]



23.38% of systems surveyed perform cybersecurity risk assessments annually. 7.61% of systems are conducting quarterly cybersecurity risk assessments and 5% of systems are conducting weekly cybersecurity risk assessments.

Risk Management Plans Addressing Cybersecurity



More than half of the systems surveyed (57.96%) have a risk management plan that addresses cybersecurity.

Risk Management Challenges

Responses varied by system type regarding risk management challenges. The **top three challenges by primary service** include:

- **Combined drinking water and wastewater systems:** 1. minimizing control system exposure; 2. assessing risks; and 3. identifying and remediation hardware or software vulnerabilities.
- **Drinking water systems:** 1. assessing risks; 2. awareness of cybersecurity threats and best practices; and 3. planning for emergencies, incidents and disasters.
- **Wastewater systems:** 1. minimizing control system exposure; 2. securing remote access to the OT system; and 3. assessing risks.

The **number one challenge** for systems serving more than 100,000 is **creating a cybersecurity culture within the utility**.

Awareness of threats and best practices was the top challenge for systems serving between 3,300 and 50,000 people.


Information-Sharing Concerns

The following high priority concerns were identified regarding the exchange of organizational information on cybersecurity threats, vulnerabilities, mitigation, and security incidents with external organizations:

ANSWER CHOICES	RESPONSES	
Lack of trust around my utility information being kept confidential	22.39%	118
Lack of credible information shared by other organizations	12.33%	65
Lack of know-how (who to share information with or how to do so)	37.76%	199
Lack of value, nothing gained in return	11.57%	61
None of the above (no barriers to information sharing with others)	30.36%	160
Don't know	16.89%	89
Total Respondents: 527		

Cybersecurity Program Challenges

Respondents gauged the extent that the following issues are a challenge for their organization's cybersecurity program. The purpose of this question was to capture elements of cybersecurity that are difficult to address.

	MINOR				SIGNIFICANT	TOTAL	WEIGHTED AVERAGE
Website security	34.78% 176	24.90% 126	21.74% 110	10.47% 53	8.10% 41	506	2.32
Information sharing	33.14% 168	21.89% 111	26.23% 133	11.83% 60	6.90% 35	507	2.37
Cloud security	28.46% 144	18.77% 95	26.09% 132	14.82% 75	11.86% 60	506	2.63
Physical security	24.11% 122	24.51% 124	26.68% 135	15.02% 76	9.68% 49	506	2.62
Incident response	19.08% 95	19.08% 95	25.90% 129	21.69% 108	14.26% 71	498	2.93
Awareness training program	18.38% 93	21.94% 111	27.67% 140	19.57% 99	12.45% 63	506	2.86
Device security	15.98% 81	23.27% 118	29.98% 152	19.33% 98	11.44% 58	507	2.87
Business continuity and disaster recovery	15.67% 79	19.05% 96	25.60% 129	20.83% 105	18.85% 95	504	3.08
Risk assessment and management	15.32% 78	18.07% 92	32.22% 164	20.04% 102	14.34% 73	509	3.00

IT- and OT-networked Assets

Information technology, or IT, refers to the business or enterprise network of a utility. This includes computers, software, firmware and similar procedures and services, such as email, websites, bill payment and customer management systems, and work order applications.

Operational technology, or OT, refers to required programmable systems that manage devices, monitor and control physical processes and events of a utility. OT includes industrial control systems, such as supervisory control and data acquisition (SCADA) systems; fire control systems; and physical access control mechanisms.

Identifying IT and OT assets is a critical first step in improving cybersecurity. An organization cannot protect what it cannot see.

37.9% of utilities have identified all IT-networked assets, with an additional 21.7% working to identify all IT-networked assets.

HAS UTILITY IDENTIFIED IT-NETWORKED ASSETS	500 or fewer	501-3,330	3,301-10,000	10,001-50,000	50,001-100,000	100,001-250,000	Greater than 250,000	Total
All IT-networked assets have been identified	1	12	12	26	44	23	30	56 204
Don't know		28	24	24	21	10	8	5 120
No work has been done to identify IT-networked assets		38	35	8	9	2	2	3 97
Work is underway to identify IT-networked assets		6	15	20	24	20	12	20 117
Total	1	84	86	78	98	55	52	84 538

30.5% of utilities have identified all OT-networked assets, with an additional 22.5% working to identify all OT-networked assets.

HAS UTILITY IDENTIFIED OT-NETWORKED ASSETS	500 or fewer	501–3,330	3,301–10,000	10,001–50,000	50,001–100,000	100,001–250,000	Greater than 250,000	Total
All OT-networked assets have been identified	1	8	9	21	35	19	31	40
Don't know		31	28	28	29	13	7	13
No work has been done to identify OT-networked assets.		40	37	9	9	3	4	1
Work is underway to identify OT-networked assets		5	12	19	25	20	10	30
Total	1	84	86	77	98	55	52	84

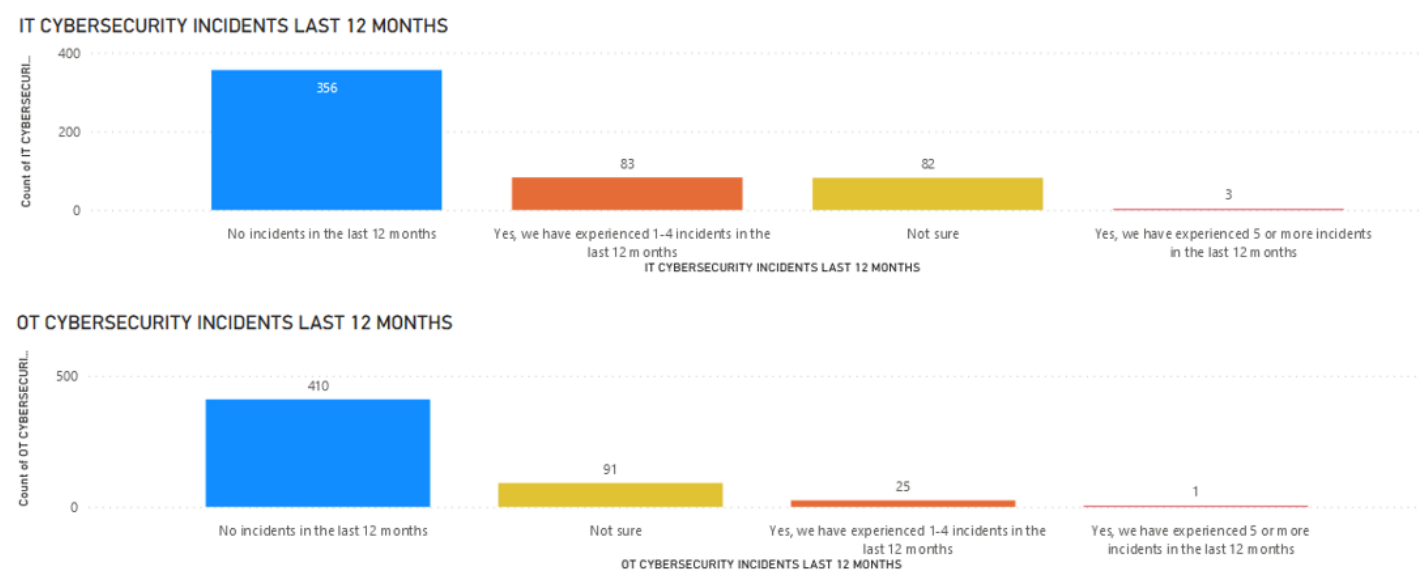
The following responses were provided in response to the question “For identified networked IT and OT assets, what is the status of your utility’s cyber protection efforts?”

Nearly 75% of respondents report they have implemented efforts or are in some stage of progress.

ANSWER CHOICES	RESPONSES	
No progress/no current plans to conduct cyber protection efforts	25.47%	135
Planning to conduct cyber protection efforts	15.47%	82
Cyber protection efforts are in progress	36.60%	194
Cyber protection efforts have been implemented and are monitored regularly	22.45%	119
TOTAL		530

IT cybersecurity incident: A violation or imminent threat of violation to the confidentiality, integrity, or availability of IT systems and/or data.

OT cybersecurity incident: A violation or imminent threat of violation to the availability, integrity, or confidentiality of OT systems and/or data.



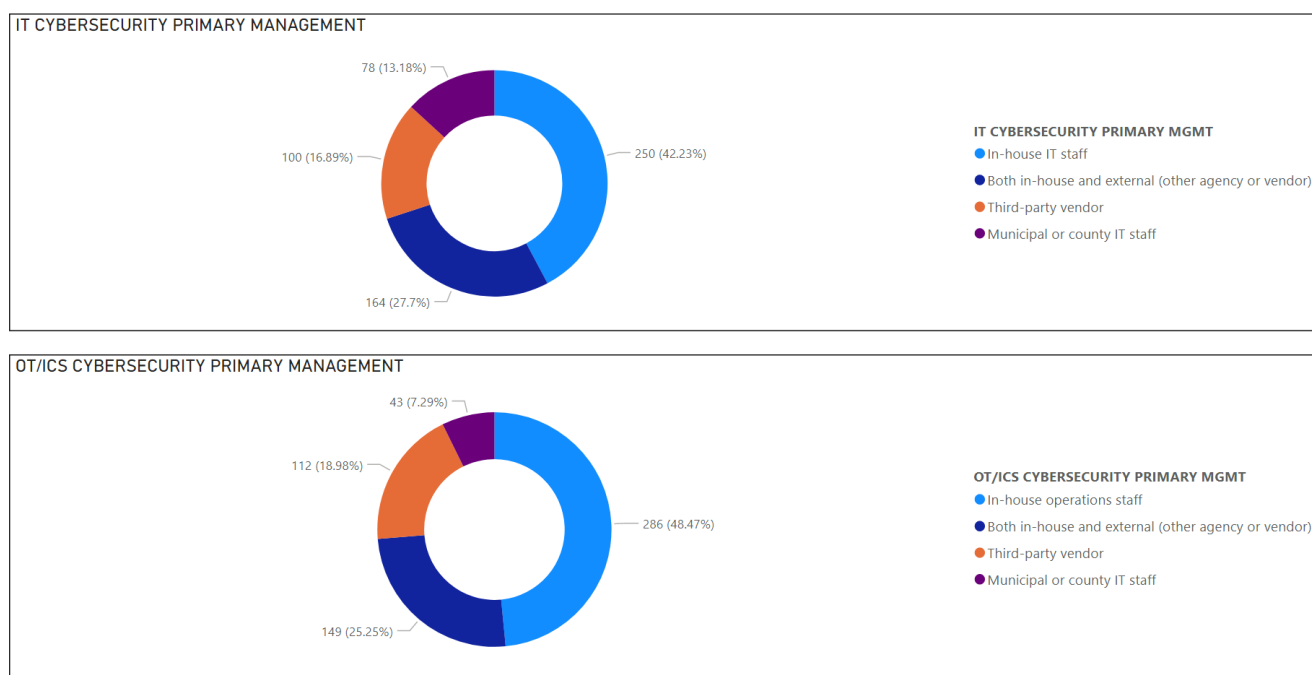
67.9% of systems reported no IT cybersecurity incidents in the last twelve months.

15.8% of systems reported having experienced 1 to 4 IT cybersecurity incidents in the last twelve months.

77.8% of systems reported no OT cybersecurity incidents in the last twelve months.

4.7% of systems reported having experienced 1 to 4 OT cybersecurity incidents in the last twelve months.

IT and OT Management and Workforce

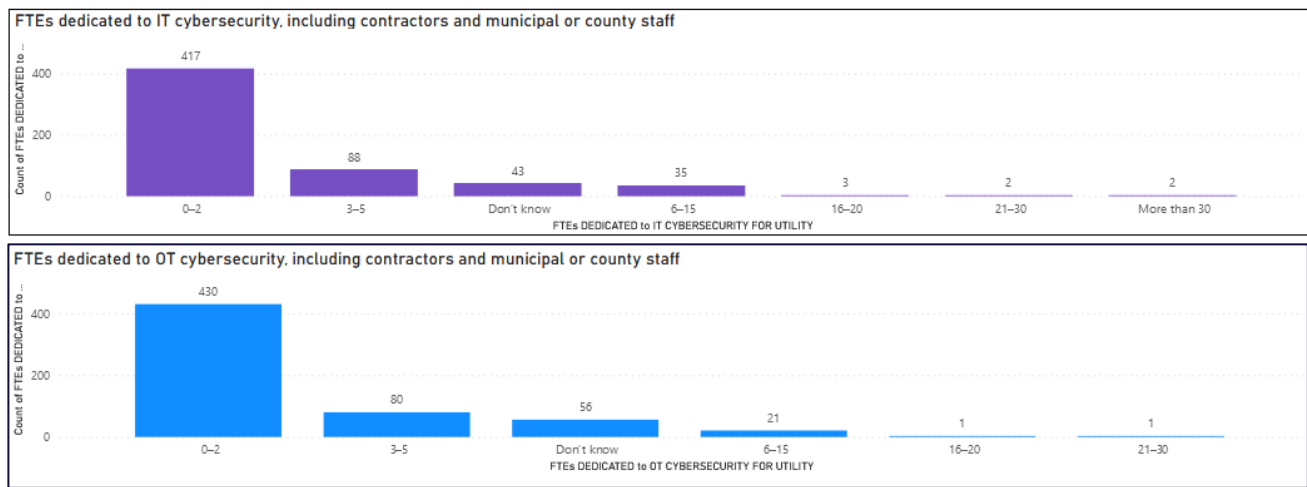


42% of utility IT cybersecurity is primarily managed by in-house IT staff. 27.7% of utility IT cybersecurity is primarily managed by both in-house and external vendors or other agencies. 16.89% of utility IT cybersecurity is primarily managed by third-party vendors. And 13.18% of utility IT cybersecurity is primarily managed by municipal or county IT staff.

48.47% of utility OT/ICS cybersecurity is primarily managed by in-house IT staff. 25.25% of utility OT/ICS cybersecurity is primarily managed by both in-house and external vendors or other agencies. 18.98% of utility OT/ICS cybersecurity is primarily managed by third-party vendors. And 7.29% of utility OT/ICS cybersecurity is primarily managed by municipal or county IT staff.

63.8% of respondents provided that their utility does not employ a Chief Information Security Officer (CISO) or equivalent. 21.9% of utilities have a CISO or equivalent. 8% of respondents noted that the role resides with their municipal or county government.

FTEs dedicated to cybersecurity include the following:

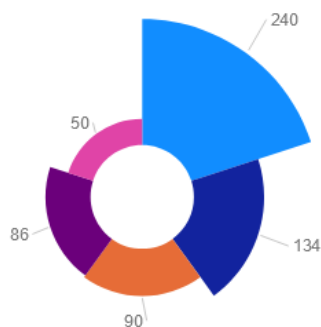


70.67% of respondents noted 0-2 FTEs dedicated to IT cybersecurity, and 73% of respondents noted 0-2 FTEs dedicated to OT cybersecurity. Additionally, the larger the utility the larger the increase in FTEs dedicated to cybersecurity.

Current Focus on Cybersecurity as a Priority

UTILITY CURRENT PRIORITY FOR CYBERSECURITY	500 or fewer	501–3,330	3,301–10,000	10,001–50,000	50,001–100,000	100,001–250,000	Greater than 250,000	Total
High	9	16	40	60	33	33	49	240
Low Priority	33	27	8	7	5	4	2	86
Medium	1	16	32	22	26	11	7	134
Not a Priority	34	8	7				1	50
Top Priority	5	14	8	18	10	9	26	90
Total	1	97	97	85	111	59	53	600

Count of UTILITY CURRENT PRIORITY FOR CYBERSECURITY



UTILITY CURRENT PRIORITY FOR CYBERSECURITY ● High ● Medium ● Top Priority ● Low Priority ● Not a Priority

55% of respondents ranked cybersecurity is a high or top priority. 22.3% consider cybersecurity a medium priority, while 22.6% - mainly systems serving 3,300 people or fewer- ranked cybersecurity a low priority or not a priority.

Cybersecurity Resources Used in the Sector

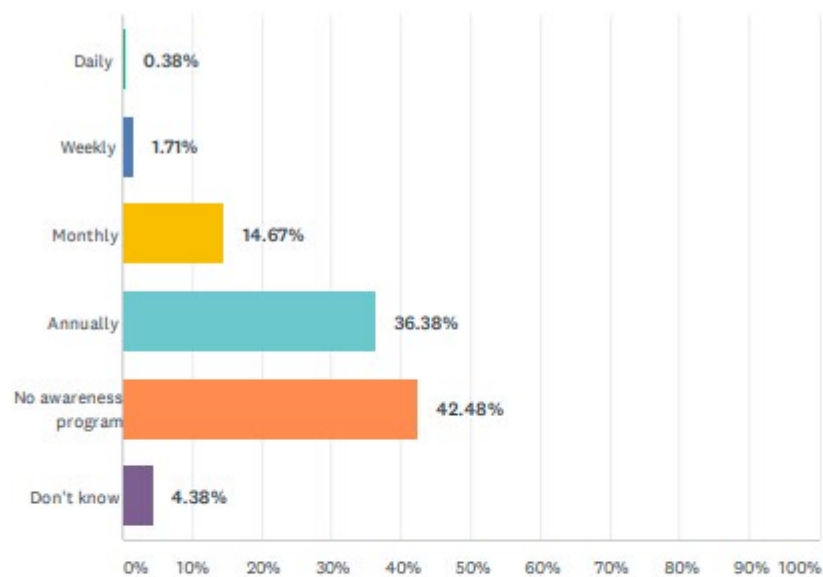
The top 5 cybersecurity resources used by utilities include the

- AWWA Cybersecurity Guidance (based on CSF)
- WaterISAC 15 Cybersecurity Fundamentals for Water and Wastewater Utilities
- NIST Cybersecurity Framework (CSF)
- DHS CISA Cybersecurity Assessment Tool (CSET) and other services
- NIST SP 800-82 Guide to Industrial Control Systems Security

Resources not covered by the survey include the U.S. Environmental Protection Agency's Cybersecurity Incident Action Checklist and its cybersecurity assessment program.

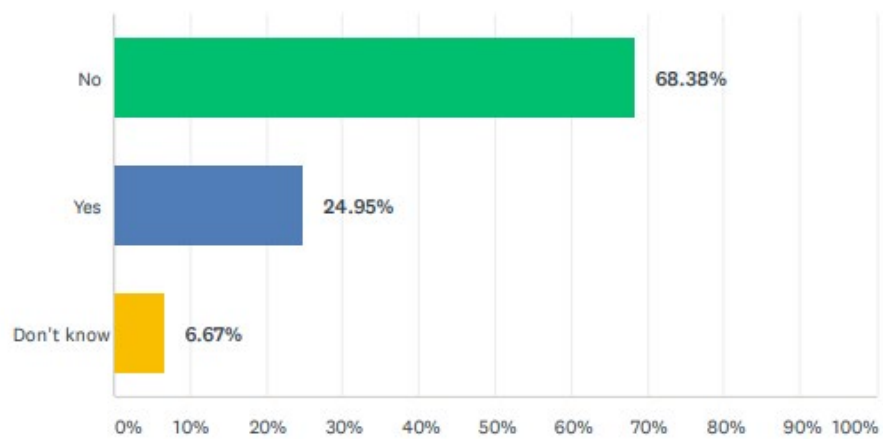
Training

More than 50% of utilities conduct cybersecurity awareness training for utility staff:



ANSWER CHOICES	RESPONSES	
Daily	0.38%	2
Weekly	1.71%	9
Monthly	14.67%	77
Annually	36.38%	191
No awareness program	42.48%	223
Don't know	4.38%	23
TOTAL		525

The following provides that nearly 25% of utilities participate in cybersecurity-related tabletop exercises, mock drills, technology failure exercises or emergency management exercises:



ANSWER CHOICES	RESPONSES	
No	68.38%	359
Yes	24.95%	131
Don't know	6.67%	35
TOTAL		525

Next Steps

Drinking water and wastewater utilities and the thousands of employees that run them are public health guardians and environmental protectors, treating drinking water to standards that meet state and federal regulations, ensuring wastewater treatment practices protect water bodies, and ensuring these vital services can continue in times of crisis.

On the whole, the sector recognizes the importance of investing in cybersecurity and adopting cybersecurity best practices. Many utilities are highly advanced, with expert IT and OT managers, keeping their devices, networks and consumers safe. Others, as shown in these results, require assistance to enhance their IT and OT cybersecurity. The sector itself also continues to support national cybersecurity efforts by collaborating with federal partners, developing its own sector-specific cybersecurity resources, and operating the Water Information Sharing and Analysis Center.

The challenges and needs outlined by respondents here offer guideposts for next steps by the Water and Wastewater Systems sector, Congress, federal agencies, and their partners.