THE ULTIMATE WATER SECTOR CYBERSECURITY PLAYBOOK

33 essential steps to safeguard your operations.

If you're running a water utility and have not implemented some of these 33 benchmarks, you're an easy target for hackers.

They see your systems as prime real estate for causing mayhem, getting paid a hefty ransom, and stealing data. If you get hacked, at the least painful end of the spectrum, you get embarrassed and have to pay out these criminals to get your systems back. At the scariest end, we're talking poisoned water or essential services not functioning for people who need it. That's what's at stake here. But by following the tips in this guide, you'll be ready to fend off these digital pirates and keep your operations smooth and secure.

Welcome to Parsons' guide to basic cybersecurity best practices. This isn't just another dull manual. These 33 steps come directly from the EPA's Water Cybersecurity Assessment Tool and Risk Mitigation Template, and we've made them easier to comprehend. As verified experts who currently serve over 600 utilities in North America, we at Parsons live and breathe this topic. We know exactly what you need to be doing and thinking about as you serve your community. Think of it as your ultimate survival guide to the wild world of cyber threats. We've taken all the dense, jargon-heavy stuff and turned it into something you'll actually enjoy reading (and hopefully take to heart).

This guide is packed with practical advice, relatable examples, and a dash of humor to keep things interesting. You don't need to be a cybersecurity expert for this to help you. In fact, if you are one, you probably don't even need this guide. This is meant for folks who know they need a stronger defense for their network but are not sure where to start.

Let's get started and turn your utility into a fortress of cyber safety.

TABLE OF CONTENTS

How to Use This Guide

All right, you've got the playbook. Now let's talk about how to use it. This guide is designed to be your step-by-step companion in bolstering your utility's cybersecurity defenses.

Step 1: Familiarize Yourself with the Basics

Start by reading through the guide to get a sense of the landscape. The 33 benchmarks are your roadmap to a more secure utility. Take note of any terms or concepts that are new to you. We've done our best to keep things clear and jargon-free, but cybersecurity does come with its own lingo.

Step 2: Assess Your Current Security Posture

Before diving into implementing changes, it's crucial to understand where you currently stand. Use the benchmarks as a checklist to evaluate your existing cybersecurity measures. This will help you identify gaps and prioritize areas that need immediate attention.

Step 3: Implement the Recommendations

Once you've assessed your current situation, start working through the guide one step at a time. Each section provides practical advice and actionable steps. Don't try to do everything at once. Cybersecurity is a marathon, not a sprint. Tackle one benchmark at a time and gradually build up your defenses.

Step 4: Document Your Progress

Keep a record of what you've implemented and when. This documentation will be invaluable, not just for tracking progress but also for demonstrating your efforts to stakeholders and auditors. Plus, it helps in ensuring that everyone on your team is on the same page.

Step 5: Regularly Review and Update

Cyber threats evolve, and so should your defenses. Set a schedule to regularly review and update your cybersecurity measures. This guide should be a living document. Revisit it periodically to ensure you're staying ahead of potential threats.

Step 6: Leverage Additional Resources

At the end of this guide, we've included a section on Parsons' cybersecurity services, including Cyberzcape and SigmaFlow. These tools can offer additional support and automation to help you maintain robust cybersecurity practices. Don't hesitate to reach out to our team for further assistance.

Final Tip: Stay Engaged and Curious

Cybersecurity isn't just a one-time effort; it's an ongoing journey. Stay engaged with the latest trends, threats, and best practices. The more you know, the better prepared you'll be to protect your utility from cyber villains.

So roll up your sleeves and let's get to work. By the time you've worked through this guide, you'll be well on your way to turning your utility into a fortress of digital safety.

Health Check – Which of the 33 Do You Do Already?

Before we dive into the nitty-gritty of making your utility pirate-proof, let's take a moment to do a quick health check. This checklist is your cybersecurity pulse check, a way to see if your defenses are rock solid or if you've got a few cracks that need patching. It's like checking the oil in your car or making sure you haven't left the back door wide open. Answer each question honestly. This isn't a test, but rather a map to guide you toward a more secure future. You'll find an expanded explanation with helpful tips on implementation (and why you should do this) for each of the 33 steps in the upcoming pages.

Cybersecurity Checklist

Use this checklist to evaluate your current cybersecurity measures. Answer each question with "Yes," "No," or "In Progress" to identify areas needing attention.

Account Security

1. Login Attempts: Do you detect and block repeated unsuccessful login attempts?
2. Default Passwords: Do you change default passwords on all devices?
3. Multi-Factor Authentication: Do you require multi-factor authentication (MFA)?
4. Password Length: Do you enforce a minimum length for passwords?
5. User and Privileged Accounts: Do you separate user and privileged accounts?
6. Unique Credentials: Do you require unique and separate credentials for OT and IT networks?
7. Account Disabling: Do you immediately disable access when it's no longer required?

Device Security

8. Software Installation Approval: Do you require approval before installing new software?
9. Macros: Do you disable Microsoft Office macros by default?
10. Asset Inventory: Do you maintain an updated inventory of OT and IT assets?
11. Unauthorized Hardware: Do you prohibit the connection of unauthorized hardware to your network?
12. Configuration Documentation: Do you document the setup and configuration settings of critical assets?

Data Security

13. Security Logs: Do you collect security logs for incident detection and investigation?
14. Log Protection: Do you protect logs from unauthorized access and tampering?
15. Encryption in Transit: Do you use effective encryption to protect data in transit?
16. Encryption at Rest: Do you use encryption to maintain the confidentiality of stored data?

Governance and Training

17. Cyber Role: Do you have a named role responsible for cybersecurity activities?
18. OT Cyber Role: Do you have a named individual responsible for OT-specific cybersecurity activities?
19. Frequency of Training: Do you provide at least annual cybersecurity training for all personnel?
20. Frequency of OT-Specific Training: Do you provide regular OT-specific cybersecurity training?
21. Information Sharing: Do you facilitate regular cybersecurity information sharing?

Vulnerability Management

22. Patching: Do you patch or otherwise mitigate known vulnerabilities within recommended time frames?
23. Internet Exposure: Do you ensure that assets connected to the public Internet expose no unnecessary services?
24. OT Internet Connections: Do you eliminate connections between OT assets and the Internet?

Supply Chain and Third Party

25. Procurement Criteria: Do you include cybersecurity as an evaluation criterion for OT and IT assets and services?
26. Vendor Notifications: Do you require vendors to notify you of security incidents or vulnerabilities?
27. Contract Clauses: Do your vendor contracts include cybersecurity clauses?

Response and Recovery

28. Incident Reporting: Do you have a written procedure for reporting cybersecurity incidents?
29. Incident Response Plan: Do you have a written cybersecurity incident response plan?
30. Backup Process: Do you back up critical systems regularly and store backups separately from source systems?
31. Network Topology: Do you maintain updated documentation of your network topology?

Other Security Measures

32. Network Segmentation: Do you segment OT and IT networks and deny connections by default unless explicitly allowed?
33. Email Security: Do you use email security controls to reduce common email-based threats like phishing and spoofing?

So, what's the verdict?

Did you find a few "No" or "In-Progress" answers lurking in your checklist? Do you have more gaps than you initially thought? That's okay. You're not alone, and you're definitely not doomed. The first step to fixing any problem is knowing it exists, and now you do. Here's how you can turn those gaps into solid defenses.

ACCOUNT SECURITY

Welcome to the heart of your utility's cybersecurity fortress: account security.

Imagine your utility as a bustling metropolis. Now, think of account security as the vigilant guardians at the gates, ensuring only the right people get in while keeping the digital baddies out. Without strong account security, it's like leaving your doors wide open with a sign that says, "Come on in!" Let's dive into the nitty-gritty of securing those accounts.

This Section Will Cover

1. **Login Attempts:** Do you detect and block repeated unsuccessful login attempts?
2. **Default Passwords:** Do you change default passwords on all devices?
3. **Multi-Factor Authentication:** Do you require multi-factor authentication (MFA)?
4. **Password Length:** Do you enforce a minimum length for passwords?
5. **User and Privileged Accounts:** Do you separate user and privileged accounts?
6. **Unique Credentials:** Do you require unique and separate credentials for OT and IT networks?
7. **Account Disabling:** Do you immediately disable access when it's no longer required?

Login Attempts

Do you detect and block repeated unsuccessful login attempts?

First up, let's talk about something that sounds simple but is crucial: detecting and blocking repeated unsuccessful login attempts. Picture this: a cybercriminal is like a determined thief trying every key on a massive keychain to break into a house. If they can keep trying keys forever, they'll eventually find the right one. This is the essence of a brute-force attack.

Now, imagine if after five wrong attempts, the lock just stops working. That's what we want to achieve here. By setting up controls to detect and block repeated failed logins, you're effectively telling those cyber thieves, "Not today, buddy!"

Why It's Important

Brute-force attacks are a common method for cybercriminals to gain access to an account. Think of it as trying every possible combination on a three-digit lock. Given enough time, they'll crack it. Computers can do this infinitely faster. Without a control to block these attempts, a hacker can try passwords endlessly until they succeed.

What to Look For

When assessing this control, here's what you should check:

- **Cybersecurity Policy:** Ensure there's a written policy that outlines the number of unsuccessful login attempts allowed before an account is locked. Typically, this number is around five or six attempts.
- **Technical Implementation:** There should be a technical policy on your system that enforces this. If someone tries to log in unsuccessfully five times, the system should automatically lock them out.

Questions to Ask

- "How many unsuccessful logins does it take before the system locks the account?"
- "Is there an alert system in place that notifies administrators of these attempts?"

By nailing down these controls, you're setting up the first line of defense against unwanted intrusions. Keep those digital doors locked tight!

Default Passwords

Do you change default passwords on all devices?

All right, next up on our cybersecurity checklist: passwords. Think of default passwords like the default settings on your TV: easy to set up but not secure for the long haul. Using default passwords is like leaving a spare key under the doormat. Everyone knows it's there, including the bad guys.

Why It's Important

Default passwords are a hacker's best friend. Many off-the-shelf devices come with factory-set passwords like "admin" or "password123." These are often listed right in the product manual or easily found online. If these passwords aren't changed, it's like giving hackers a map straight into your network. Changing these passwords is the first step in kicking them to the curb.

What to Look For

When checking if a utility has this control in place, here's what you should focus on:

- **Written Policy:** The utility should have a policy that mandates changing default passwords on all new devices before they are connected to the network.
- **Responsibility Assignment:** Someone needs to be clearly responsible for ensuring this happens every time a new asset is added to the network.

Questions to Ask

- "Do you have a written policy that requires changing default passwords?"
- "Is there a specific person or team responsible for changing default passwords on new devices?"

Changing default passwords isn't just a good idea; it's essential. It's like putting a deadbolt on your door instead of relying on a flimsy latch. Make sure those passwords are unique and strong to keep the intruders out.

Multi-Factor Authentication

Do you require multi-factor authentication (MFA)?

Now let's talk about a superhero of the cybersecurity world: multi-factor authentication (MFA). If passwords are the bouncers at your utility's digital nightclub, MFA is like adding a VIP list and a retina scanner at the door. It's an extra layer that ensures only the right people get in, even if someone sneaks past the first guard.

Why It's Important

MFA adds a crucial second step to the login process. Even if a cyber villain gets ahold of a password, they'll hit a wall when asked for a second form of identification. Think of it this way: you can know the password (something you know), but you also need to have something like a smartphone app that generates a one-time code (something you have). This makes it exponentially harder for the bad guys to get in.

The stats don't lie: the FBI Cyber Division found that 99.9% of hacked accounts they investigated didn't use MFA. That's like leaving your front door wide open and being surprised when someone walks in.

What to Look For

When checking for MFA implementation, focus on these aspects:

- **Cybersecurity Policy:** There should be a policy requiring MFA for at least remote access to operational technology (OT) networks.
- **Technical Demonstration:** Ideally, the utility can demonstrate how MFA is implemented. They might show how logging into their OT network requires a second authentication factor, like a code sent to a smartphone.

Questions to Ask

- "Can you show me how MFA works when accessing the OT network remotely?"
- "Which MFA vendor or solution do you use?"

Seeing MFA in action is like watching a superhero at work: it's impressive and incredibly reassuring. By making MFA a standard practice, you're putting up a formidable defense that even the craftiest cybercriminals will struggle to bypass.

Password Length

Do you enforce a minimum length for passwords?

Next on our cybersecurity journey: the length of your passwords. Think of short passwords like flimsy, outdated locks. They might keep out casual snoopers, but serious intruders will laugh as they walk right through. We need to upgrade those locks to something that can withstand a serious assault.

Why It's Important

Modern attacker tools can crack an eight-character password almost instantly. That's not hyperbole; I've seen it firsthand in cybersecurity labs. On the flip side, a 15-character password, even one with just lowercase letters, can take these tools an estimated 1,000 years to crack. That's like comparing a rickety wooden door to a titanium vault.

What to Look For

When assessing this control, here's what you should verify:

- **Written Policy:** The utility should have a policy that sets a minimum password length requirement. Ideally, this would be at least 15 characters.
- **Technical Enforcement:** There should be a system-enforced policy that rejects passwords shorter than the required length. If a utility staff member tries to use a password that's too short, the system should kick it back with a firm "nope."

Questions to Ask

- "Do you have a policy that specifies the minimum length for passwords?"
- "Is there a technical control in place that enforces this minimum length?"

Educating employees about the importance of longer passwords is also crucial. Even if they don't have a technical enforcement policy, ensuring everyone understands why longer passwords matter can make a big difference. Think of it as teaching them to build better locks for their digital doors.

By setting and enforcing a minimum password length, you're making it much harder for cybercriminals to barge in. Let's make sure those passwords are long, strong, and ready to take on any threat.

User and Privileged Accounts

Do you separate user and privileged accounts?

Now let's move on to separating user and privileged accounts. Think of privileged accounts like the master keys to your entire utility. You wouldn't hand out master keys to everyone, would you? The same goes for administrator accounts. Only the right people should have access to these powerful tools.

Why It's Important

Administrator accounts have full control over your system. If a cybercriminal gets their hands on one, they can wreak havoc. They can change settings, access sensitive data, and generally cause mayhem. Separating user accounts from privileged accounts is like making sure only the trusted few have the keys to the kingdom.

What to Look For

When checking if a utility has this control in place, here's what you should focus on:

- **Updated List of Admin Accounts:** The utility should maintain an updated list of all users with administrator access. This helps in monitoring and auditing who has the keys to the castle.
- **Policy and Technical Controls:** Ideally, there should be policies and technical controls in place that prevent users from using the same password for both their user and administrator accounts.

Questions to Ask

- "Do you have an updated list of all users with administrator access?"
- "How often do you evaluate and reevaluate administrator account privileges?"

Evaluating admin accounts periodically ensures that only those who really need these privileges have them. For example, someone might need admin access temporarily for a project, but once it's done, their access should be revoked. It's about keeping the master keys secure and limited to those who genuinely need them.

By separating user and privileged accounts, you're making it much harder for cybercriminals to gain full control of your systems. Keep those master keys safe and ensure only the trusted few have access.

Unique Credentials

Do you require unique and separate credentials for OT and IT networks?

Next up, we're talking about unique and separate credentials for accessing OT and IT networks. Think of this as having separate keys for different doors in your utility. You wouldn't use the same key for the front door and the vault, right? The same logic applies here. Separate credentials add an extra layer of security.

Why It's Important

If an attacker gets ahold of a user's IT credentials, the last thing you want is for them to use those same credentials to waltz into the OT network and cause chaos. Having unique and separate credentials for OT and IT networks means that even if one set is compromised, the other remains secure. It's about compartmentalizing access to limit potential damage.

What to Look For

When assessing this control, here's what you should check:

- **Cybersecurity Policy:** There should be a policy that mandates the use of unique and separate credentials for OT and IT networks.
- **Employee Education:** Employees should be educated about the importance of using different credentials for different networks.

Questions to Ask

- "Do you have a policy requiring separate credentials for OT and IT networks?"
- "Are employees educated on the importance of using different credentials for different networks?"

More advanced utilities might even have technical controls in place that prevent the same password from being used across OT and IT networks. But at the very least, having a written policy and educating employees about the risks of using the same credentials are crucial.

By requiring unique and separate credentials, you're adding an important layer of security that helps protect your utility's most critical systems from being compromised. Keep those keys separate to keep the bad guys out.

Account Disabling

Do you immediately disable access when it's no longer required?

Finally, let's talk about the importance of immediately disabling access when it's no longer needed. Think of inactive accounts like unguarded doors. Even if they seem harmless, they can become entry points for cyber mischief if not properly managed. When someone leaves your utility or changes roles, their access should be cut off faster than a speeding ticket.

Why It's Important

Inactive accounts are a favorite target for cyber attackers. They can exploit these accounts without raising red flags, slipping in unnoticed. Disabling access immediately upon an employee's departure or role change also protects against insider threats. Imagine a disgruntled former employee still having access to critical systems—it's a recipe for disaster.

What to Look For

When checking if a utility has this control in place, focus on:

- **Administrative Process:** There should be a defined and enforced process for disabling access. This process should ensure that all accounts are disabled the same day an employee leaves or changes roles.
- **Responsibility Assignment:** Someone needs to be responsible for following this process every time. It's not just about having a policy; it's about ensuring it's executed without fail.

Questions to Ask

- "Do you have a process for disabling access on the day an employee leaves or changes roles?"
- "Is there a specific person or team responsible for ensuring this process is followed?"

Think of this as locking the doors as soon as someone leaves the building. It prevents unauthorized access and keeps your systems secure. It's not just about cybersecurity; it's about maintaining trust and integrity within your utility.

By immediately disabling access when it's no longer needed, you're closing potential back doors that cybercriminals might use to infiltrate your systems. Make sure those doors are locked tight and only open for the right people.

DEVICE SECURITY

Onto the next level of our cybersecurity journey: device security.

Think of this as fortifying every gadget, gizmo, and machine within your utility. From the industrial control systems monitoring water treatment to the laptops used for daily admin tasks, every device is a potential doorway for cyber villains. Securing these devices is like installing high-tech locks and surveillance on every door and window of your digital house. Let's dive into the details and lock those doors tight.

This Section Will Cover

8. **Software Installation Approval:** Do you require approval before installing new software?
9. **Macros:** Do you disable Microsoft Office macros by default?
10. **Asset Inventory:** Do you maintain an updated inventory of OT and IT assets?
11. **Unauthorized Hardware:** Do you prohibit the connection of unauthorized hardware to your network?
12. **Configuration Documentation:** Do you document the setup and configuration settings of critical assets?

Software Installation Approval

Do you require approval before installing new software?

First up, let's talk about software installation. Picture this: an attacker disguises malicious software to look like the latest productivity app. Without a proper approval process, anyone could download it, unwittingly inviting a cyber threat into your network. Requiring approval before installing new software is like having a vigilant gatekeeper who scrutinizes every package before it's let inside.

Why It's Important

Cybercriminals often disguise malicious software to look like legitimate applications. Without an approval process, employees might download harmful software that compromises your system. Having an approval process ensures that only safe, vetted software is installed, reducing the risk of introducing malware into your network.

What to Look For

When evaluating this control, here's what you should verify:

- **Written Policy:** There should be a clear, enforced policy outlining the approval process for software installation. This isn't the Wild West. Not every piece of software should get a free pass.
- **Approved Software List:** Maintaining a risk-informed list of pre-approved software can streamline the process while keeping security tight. For instance, the EPA has a list of software that can be downloaded without additional approval. Utilities should consider a similar approach.

Questions to Ask

- "Can you explain your software approval process?"
- "Are employees limited on what software they can download on utility assets?"

Ensuring that only approved software makes it onto your devices is crucial. It's like having a top-tier bouncer at a club, making sure only the right people get in and keeping troublemakers out.

Macros

Do you disable Microsoft Office macros by default?

Let's talk Microsoft Office macros and embedded code. These little snippets of code are designed to make your life easier, but in the hands of cybercriminals, they can turn into a Trojan horse, wreaking havoc on your system. Disabling macros by default is like setting up a moat around your castle. It keeps the bad stuff out while letting the good stuff in only when necessary.

Why It's Important

Macros can be incredibly useful, automating tasks and improving efficiency. However, they can also be weaponized by cybercriminals to run malicious code as soon as a document is opened. By disabling macros by default, you prevent these malicious scripts from running automatically, reducing the risk of a cyberattack.

What to Look For

When assessing this control, here's what you should check:

- **Written Policy:** Ensure there's a cybersecurity policy that enforces the disabling of macros on all utility assets. This should be a default setting to block any potentially harmful macros from executing.
- **Request Process:** There should be a clear process for users to request enabling macros when they are genuinely needed. This process ensures that macros are only enabled after proper scrutiny.

Questions to Ask

- "Do you have a policy or procedure for users to submit a request to enable macros if or when they are needed?"
- "How do you handle documents that require macros for functionality?"

By default, disabling macros adds a vital layer of security, preventing malicious code from sneaking in through seemingly harmless documents. It's like having a guard dog that barks at unknown visitors but knows when to let the trusted mailman in.

Asset Inventory

Do you maintain an updated inventory of OT and IT assets?

Now let's talk about keeping an inventory of all your OT and IT assets. Imagine trying to protect a treasure chest without knowing what's inside it. Sounds risky, right? The same goes for your utility's devices. You can't secure what you don't know you have. Maintaining an updated inventory is the foundation of a solid cybersecurity strategy.

Why It's Important

You need to know what assets you have to protect them effectively. Without a comprehensive inventory, vulnerabilities can go unnoticed, and patches might not be applied where needed. It's like trying to insure your car without knowing its make, model, or value. You can't protect it if you don't know what you have.

What to Look For

When evaluating this control, here's what you should check:

- **Physical or Digital Inventory List:** The utility should maintain an updated list of all OT and IT assets. This list should include every device on the network, from industrial control systems to laptops.
- **Regular Updates:** The inventory should be reviewed and updated regularly, especially when new assets are added or old ones are decommissioned.

Questions to Ask

1. "Do you maintain an updated inventory of all OT and IT assets?"
2. "How often do you review and update this inventory list?"

A well-maintained inventory list is essential for tracking vulnerabilities and ensuring all assets are accounted for. It's like having a detailed map of your treasure. You know exactly what you have and where it's located, making it much easier to protect.

Unauthorized Hardware

Do you prohibit the connection of unauthorized hardware to your network?

Next on our device security checklist is controlling the connection of unauthorized hardware. Picture this: your utility is a high-security facility, and plugging in unauthorized hardware is like allowing random gadgets into the control room. It's a risk you can't afford to take. Cybercriminals often exploit these loose ends to sneak malware into your network.

Why It's Important

Malicious USB drives and other unauthorized hardware can be used to introduce malware and cause breaches. Cybercriminals might "drop" infected USB drives around your facility, hoping someone will pick one up and plug it in. This method, known as a "baiting attack," can lead to severe security breaches. Disabling unused USB ports and prohibiting unauthorized hardware connections are essential steps to mitigate this risk.

What to Look For

When evaluating this control, focus on the following:

1. **Administrative Policy:** There should be a written policy banning the use of unauthorized hardware, such as USB drives, on OT and IT assets. This policy should be enforced rigorously.
2. **Technical Controls:** If possible, USB ports should be disabled on devices that don't need them, and physical measures like port blockers can be used.

Questions to Ask

- "Do you have a written policy that prohibits the use of unauthorized hardware?"
- "How does your utility protect against unauthorized hardware connections?"
- "Are USB ports disabled on devices that do not require them?"

Implementing strict controls on hardware connections is like having a metal detector at the entrance. It ensures that nothing harmful makes its way into your secure environment. By being vigilant about what gets plugged into your network, you're adding a critical layer of defense against potential cyber threats.

Configuration Documentation

Do you document the setup and configuration settings of critical assets?

Finally, let's talk about the importance of documenting the setup and configuration settings of your critical OT and IT assets. Imagine trying to fix a high-tech gadget without a user manual. It's a recipe for frustration and potential disaster. Keeping detailed records of how your systems are configured helps ensure that you can manage, maintain, and secure them effectively.

Why It's Important

Having current documentation of your system configurations is crucial for several reasons. It allows you to quickly identify which assets might be vulnerable to newly discovered threats, streamline troubleshooting, and ensure consistency across your network. For example, when the Log4J vulnerability surfaced, utilities with detailed configuration records could swiftly identify affected systems and apply necessary patches.

What to Look For

When assessing this control, here's what you should verify:

- **Configuration Documentation:** The utility should maintain updated documentation detailing the setup and configuration of all critical OT and IT assets. This includes patch levels, software versions, and specific configuration settings.
- **Regular Reviews:** Ensure that this documentation is reviewed and updated regularly to reflect any changes in the system configurations.

Questions to Ask

- "Do you have current documentation detailing the setup and settings of your critical OT and IT assets?"
- "How often do you review and update this configuration documentation?"

This documentation can be an extension of the asset inventory, adding a column for configuration details. Keeping this information up to date is like having a detailed user manual for your entire network. It makes managing and securing your systems much more efficient.

By maintaining comprehensive documentation of your system setups and configurations, you're ensuring that you can quickly and effectively respond to vulnerabilities and changes. It's all about having the right information at your fingertips when you need it most.

DATA SECURITY

The lifeblood of your utility's operations is data security. This control family is all about the CIA triad: **C**onfidentiality, **I**ntegrity, and **A**vailability. It might sound like a spy thriller, but it's the bedrock of keeping your data safe from prying eyes and malicious hands. Utilities handle a ton of data, from employee and customer personally identifiable information (PII) to billing details and passwords. Imagine this data as precious cargo that you definitely don't want to fall into the wrong hands, especially cybercriminals.

Ensuring the security of this data isn't just about putting up barriers; it's about maintaining the trust and reliability that your utility stands for. Picture your data as a treasure chest. You need strong locks (encryption), vigilant guards (logging and monitoring), and a fortress (secure storage) to keep it safe. Let's break down the key steps to make sure your data remains secure and out of reach of digital pirates.

This Section Will Cover

13. **Security Logs:** Do you collect security logs for incident detection and investigation?
14. **Log Protection:** Do you protect logs from unauthorized access and tampering?
15. **Encryption in Transit:** Do you use effective encryption to protect data in transit?
16. **Encryption at Rest:** Do you use encryption to maintain the confidentiality of stored data?

Security Logs

Do you collect security logs for incident detection and investigation?

First up, let's talk about security logs. Think of these logs as the security cameras of your digital world. They record what happens within your OT and IT systems, providing vital clues if someone tries to mess with your setup.

Why It's Important

Logs help you detect and investigate incidents. They can reveal if you're about to become a victim of a cyberattack or if you've already been compromised. Without logs, it's like running a business without security cameras. You'd have no idea who's been sneaking around. They provide the written evidence you need to understand what happened, how severe it was, and maybe even who did it.

What to Look For

When assessing this control, here's what you should verify:

- **Logging Procedures:** The utility should have a process for collecting logs. This includes details about what systems are logged and how the logs are collected.
- **Standard Operating Procedures:** Documentation that outlines the logging process should be part of the utility's cybersecurity policy.

Questions to Ask

- "Do you collect security logs? If so, what is your logging process and procedures?"
- "Can you explain what types of events you log?"

Even small utilities can implement simple logging solutions, like recording login activities. Whether it's logging complex events or just keeping track of login attempts, every bit helps in creating a secure environment.

Log Protection

Do you protect logs from unauthorized access and tampering?

Next, let's ensure those precious logs are protected from unauthorized access and tampering. Imagine an attacker breaking into your system and wiping the logs clean. It's like deleting the security footage after a heist. Protecting logs ensures you have the evidence you need to respond effectively to an attack.

Why It's Important

If an attacker can delete logs, they can cover their tracks, making it incredibly difficult to investigate and respond to a cyber incident. Protecting logs is essential to maintain the integrity of your incident response process. It's like having a backup copy of your security footage stored in a secure location.

What to Look For

When evaluating this control, focus on:

- **Backup Procedures:** Logs should be backed up regularly and stored securely, ideally on a separate server.
- **Security Measures:** Ensure there are safeguards in place to prevent unauthorized access to logs.

Questions to Ask

- "How often do you check and back up your logs?"
- "What safeguards do you have in place to protect your logs from tampering?"

Effective log protection involves regular backups and secure storage solutions. This way, even if your main server is compromised, you have a secure copy of your logs to fall back on.

Encryption in Transit

Do you use effective encryption to protect data in transit?

Moving on, let's talk about encryption for data in transit. Picture data in transit like a letter being sent through the mail. Without encryption, anyone could intercept and read it. Encryption ensures that even if the letter is intercepted, it remains unreadable to unauthorized eyes.

Why It's Important

Encryption protects the confidentiality of data as it travels across networks. This ensures that sensitive information isn't exposed to prying eyes during transmission. It's like sealing your letter in a tamper-proof envelope: only the intended recipient can read it.

What to Look For

When assessing this control, verify:

- **Encryption Procedures:** There should be a documented process for encrypting data in transit, detailed in the utility's cybersecurity policy.
- **Types of Encryption Used:** Ensure that the encryption methods used are robust and up to date.

Questions to Ask

- "How do you ensure data in transit is encrypted?"
- "What encryption methods do you use?"

Encryption of data in transit is a critical step in safeguarding sensitive information. Make sure the utility employs strong encryption methods to keep data secure as it moves through cyberspace.

Encryption at Rest

Do you use encryption to maintain the confidentiality of stored data?

Finally, let's address encryption for data at rest. Imagine storing a sensitive letter in a filing cabinet. If someone breaks into your house and opens the cabinet, they can read it, unless it's encrypted. Encrypting stored data ensures that even if cybercriminals get their hands on it, they can't read it.

Why It's Important

Encrypting stored data protects it from unauthorized access. Even if a cybercriminal gains physical access to your storage devices, they won't be able to read the encrypted data. It's like locking your filing cabinet and then hiding the key.

What to Look For

When assessing this control, verify:

- **Encryption Policies:** The utility should have a policy that mandates encryption for all stored sensitive data detailed in their cybersecurity policy.
- **Implementation of Encryption Tools:** Ensure the utility uses effective encryption tools for data at rest, such as BitLocker or similar solutions.

Questions to Ask

- "How do you ensure that stored data is encrypted?"
- "What encryption tools do you use for data at rest?"

Encrypting stored data adds a vital layer of security, protecting sensitive information from being accessed even if physical security is breached. Make sure the utility employs robust encryption practices to safeguard their data.

GOVERNANCE AND TRAINING

Welcome to the fourth control family: governance and training. This section is all about ensuring your utility has the leadership and training necessary to foster a culture of cybersecurity. Imagine building a strong and resilient cybersecurity program like constructing a skyscraper. You need a solid foundation, skilled workers, and constant vigilance to keep it standing tall. Proper governance and regular training are the blueprints and practice drills that ensure everyone knows their role in keeping your utility secure.

Governance involves having clear leadership and accountability for cybersecurity, while training ensures everyone in the utility is prepared to face cyber threats head on. Think of cybersecurity training as regular workouts for your digital muscles, keeping them strong and ready for any challenge. From basic cybersecurity 101 to simulated phishing tests, there are plenty of ways to keep your team sharp. Let's dive into the specifics.

This Section Will Cover

17. **Cyber Role:** Do you have a named role responsible for cybersecurity activities?
18. **OT Cyber Role:** Do you have a named individual responsible for OT-specific cybersecurity activities?
19. **Frequency of Training:** Do you provide at least annual cybersecurity training for all personnel?
20. **Frequency of OT-Specific Training:** Do you provide regular OT-specific cybersecurity training?
21. **Information Sharing:** Do you facilitate regular cybersecurity information sharing?

Cyber Role

Do you have a named role responsible for cybersecurity activities?

First up, let's talk about the importance of having a named role for cybersecurity activities. Think of this person as the captain of your cybersecurity ship. They don't need to be a cybersecurity expert, but they do need to be the go-to decision-maker for all things cyber.

Why It's Important

Having a designated individual responsible for cybersecurity ensures there's always someone steering the ship. This person can lead training, plan exercises, and advocate for cybersecurity resources. They're the point person who makes sure cybersecurity is a priority and not just an afterthought.

What to Look For

When assessing this control, here's what you should verify:

- **Named Individual:** The utility should be able to identify the person responsible for cybersecurity.
- **Documented Duties:** There should be clear documentation of this individual's roles and responsibilities.

Questions to Ask

- "Do you have a named individual responsible for cybersecurity?"
- "Can you explain the roles and responsibilities of your cybersecurity lead?"

Having a clear leader for cybersecurity activities ensures that someone is always focused on maintaining and improving your utility's defenses. It's like having a coach who keeps the team motivated and on track.

OT Cyber Role

Do you have a named individual responsible for OT-specific cybersecurity activities?

Now let's turn our attention to the operational technology (OT) side. Just like the overall cybersecurity lead, it's crucial to have someone specifically responsible for OT cybersecurity. Think of this person as the specialist who understands the unique needs and challenges of your OT systems.

Why It's Important

OT systems have distinct cybersecurity requirements that differ from IT systems. Having a dedicated individual for OT cybersecurity ensures these unique needs are addressed. This person can focus on the specific threats and vulnerabilities that OT systems face.

What to Look For

When evaluating this control, verify:

- **Named Individual for OT:** The utility should be able to identify the person responsible for OT cybersecurity. This can be the same person as the overall cybersecurity lead or a different individual.
- **Documented Duties:** There should be clear documentation of this individual's roles and responsibilities related to OT cybersecurity.

Questions to Ask

- "Do you have a named individual responsible for OT cybersecurity?"
- "Are the roles and responsibilities of this OT lead different from the overall cybersecurity lead? How so?"

Having a dedicated OT cybersecurity lead ensures the unique security needs of your operational technology are not overlooked. It's like having a specialist doctor who knows exactly how to treat specific ailments.

Frequency of Training

Do you provide at least annual cybersecurity training for all personnel?

Next, let's focus on the frequency of training. Regular training is like a vaccination against cyber threats. It prepares your team to recognize and respond to potential attacks before they can do harm.

Why It's Important

Regular, basic cybersecurity training is essential for building a cybersecurity-aware culture. Training helps employees recognize potential threats and respond quickly and appropriately. Frequent training ensures that everyone stays up to date with the latest threats and best practices.

What to Look For

When assessing this control, verify:

- **Training Schedules and Records:** The utility should have documented records of cybersecurity training sessions, ensuring they occur at least annually.
- **Training Content:** Ensure the training covers basic cybersecurity concepts relevant to all employees.

Questions to Ask

- "Do all employees receive cybersecurity training at least annually?"
- "What topics are covered in your cybersecurity training?"
- "How do you ensure that all employees complete the training?"

By providing regular training, you're building a workforce that's vigilant and prepared to handle cyber threats. It's like giving your team a regular workout to keep their cyber muscles in shape.

Frequency of OT-Specific Training

Do you provide regular OT-specific cybersecurity training?

Moving on, let's talk about OT-specific cybersecurity training. Just like regular training, this is crucial, but with a focus on the unique aspects of operational technology.

Why It's Important

OT systems face distinct cybersecurity challenges that require specialized training. Employees working directly with OT need to understand these unique threats and how to address them. Regular OT-specific training ensures they're prepared to protect these critical systems.

What to Look For

When evaluating this control, verify:

- **Training Schedules and Records:** Ensure there's a documented schedule for OT-specific cybersecurity training.
- **Training Content:** Verify that the training is tailored to the unique aspects of OT cybersecurity.

Questions to Ask

- "Do all employees who work with OT receive specialized cybersecurity training?"
- "How is this OT-specific training different from the basic cybersecurity training?"

By providing regular OT-specific training, you're ensuring that those who work directly with your critical systems are well prepared to protect them. It's like giving specialized training to your elite task force.

Information Sharing

Do you facilitate regular cybersecurity information sharing?

Finally, let's discuss the importance of regular cyber information sharing. Breaking down silos between OT and IT departments is crucial for a cohesive cybersecurity strategy.

Why It's Important

Effective communication and coordination between OT and IT personnel ensure that everyone is on the same page regarding cybersecurity. Regular meetings help break down barriers and align priorities, reducing the risk of vulnerabilities falling through the cracks.

What to Look For

When evaluating this control, verify:

- **Meeting Records and Agendas:** Documentation of regular meetings between OT and IT personnel, including vendors if applicable.
- **Coordination Efforts:** Evidence of efforts to foster communication and coordination between these groups.

Questions to Ask

- "Do you hold regular meetings to discuss cybersecurity with both OT and IT personnel?"
- "How do you ensure these meetings foster meaningful relationships and effective communication?"

Regular cyber information sharing is like having a team huddle before a big game. It ensures everyone knows the game plan and works together seamlessly.

VULNERABILITY MANAGEMENT

Think of this as your utility's regular home inspection. Just as you'd check your house for security risks, ensuring doors are locked, alarms are set, and windows are fixed, vulnerability management involves identifying and fixing weaknesses in your computer systems and software to prevent cyber attackers from exploiting them. It's all about staying vigilant and proactive to keep your operations running smoothly.

Vulnerability management ensures that vulnerabilities are mitigated in a timely manner and that you stay updated on the latest threats that could impact your utility. From zero-day vulnerabilities and software flaws to exposed ports and interconnected OT and IT assets, there are plenty of potential entry points for cyber villains. Let's break down how to keep your digital house in order.

This Section Will Cover

22. **Patching:** Do you patch or otherwise mitigate known vulnerabilities within recommended time frames?
23. **Internet Exposure:** Do you ensure that assets connected to the public Internet expose no unnecessary services?
24. **OT Internet Connections:** Do you eliminate connections between OT assets and the Internet?

Patching

Do you patch or otherwise mitigate known vulnerabilities within recommended time frames?

First up, let's talk about patching. Imagine finding a crack in your house's foundation. You wouldn't leave it unattended, right? The same goes for vulnerabilities in your software and hardware. Cybercriminals are constantly on the lookout for these cracks to exploit.

Why It's Important

Vulnerabilities are weaknesses that can be exploited by cyber attackers to launch attacks. Keeping your systems patched ensures these weaknesses are fixed before they can be exploited. The Log4J vulnerability is a prime example of a critical flaw that continues to be exploited due to unpatched software.

What to Look For

When assessing this control, here's what you should verify:

- **Updated Asset Inventory:** Ensure the utility maintains an updated inventory of all assets, which helps in identifying vulnerabilities.
- **Evidence of Vulnerability Scans:** Look for documentation of recent vulnerability scans, such as those conducted for free by CISA.

Questions to Ask

- "Do you have a method to stay up to date on the latest vulnerabilities?"
- "Do you have a procedure for mitigating known vulnerabilities within a certain time frame?"
- "Do you attend cybersecurity conferences, sign up for cyber newsletters, or utilize free online resources to stay informed?"

Staying on top of patches and updates is crucial for maintaining a secure environment. It's like regularly checking and fixing any structural issues in your home to keep it safe and sound.

Internet Exposure

Do you ensure that assets connected to the public Internet expose no unnecessary services?

Next, let's ensure your digital doors aren't left wide open. Just as you wouldn't leave your front door unlocked for anyone to walk in, you shouldn't leave unnecessary exploitable services exposed to the public Internet.

Why It's Important

Ports are how computers communicate and provide services over the Internet. If left open and unsecured, these ports can serve as entry points for attackers. Ensuring that only necessary services are exposed reduces the risk of unauthorized access.

What to Look For

When evaluating this control, verify:

- **Vulnerability Scan Results:** Look for documentation from recent vulnerability scans, such as those offered by CISA.
- **Standard Operating Procedures (SOPs):** Check for SOPs that outline compensating controls for necessary open ports.

Questions to Ask

- "How do you ensure vulnerable ports are not left open at your utility, or how are they protected when they must be left open?"

Implementing compensating controls, like motion sensors or security lights for digital entry points, helps protect your utility's network. It's about ensuring that even if you must leave a digital door open, you have measures in place to monitor and secure it.

OT Internet Connections

Do you eliminate connections between OT assets and the Internet?

Now, let's address connections between OT assets and the Internet. Think of your operational technology like the essential utilities in your home: your hot water heater or HVAC system. You wouldn't want someone randomly turning off your hot water or adjusting your thermostat from afar.

Why It's Important

OT systems such as SCADA, ICS, or PLCs were not designed with security in mind and can be vulnerable when connected to the Internet. Removing unnecessary Internet connections minimizes the risk of these critical systems being exploited by cyber attackers.

What to Look For

When assessing this control, verify:

- **Vulnerability Scan Results:** Review recent scan results to identify any OT assets connected to the Internet.
- **SOPs for OT Internet Connections:** Check for SOPs that justify and document the need for any OT asset to be connected to the Internet.

Questions to Ask

- "Does your OT cybersecurity lead approve or deny requests to connect OT assets to the Internet?"

Ensuring that OT assets are not unnecessarily connected to the Internet is like making sure your home's critical systems are secure and only accessible to those who need them. It's about protecting the heart of your utility's operations from cyber threats.

SUPPLY CHAIN AND THIRD-PARTY MANAGEMENT

Think of supply chain and third-party management as deciding who to invite into your home. You wouldn't let just anyone walk through your front door. You want to make sure they're trustworthy and won't cause any trouble. The same goes for your utility's interactions with vendors and third parties. It's crucial to ensure they have robust cybersecurity practices to prevent inadvertently introducing cyber risks into your environment.

When companies work together or use services from other companies, it's essential to check if these partners have solid cybersecurity measures in place. Utilities need to ensure that they won't accidentally bring in cyber problems that could harm their processes or systems. Securing the supply chain involves asking vendors about their cybersecurity practices and including specific cybersecurity requirements in contract language.

This Section Will Cover

25. **Procurement Criteria**: Do you include cybersecurity as an evaluation criterion for OT and IT assets and services?
26. **Vendor Notifications:** Do you require vendors to notify you of security incidents or vulnerabilities?
27. **Contract Clauses:** Do your vendor contracts include cybersecurity clauses?

Procurement Criteria

Do you include cybersecurity as an evaluation criterion for OT and IT assets and services?

First up, let's talk about including cybersecurity as a criterion for procurement. Think of this like car shopping. You wouldn't just pick a car based on looks and speed. You'd also consider safety features like crash-test ratings and airbags. Similarly, when a utility buys new technology, it's important to ensure it's safe from cyber threats.

Why It's Important

Installed hardware and software may have unintentional weaknesses that cyber attackers can exploit to enter a system or network. By including cybersecurity requirements in the procurement process for OT and IT assets, utilities can better understand which vendors offer the most secure services.

What to Look For

When assessing this control, verify:

- **Procurement Language:** Check for language in solicitations and contracts that requires bidders to include information on their cybersecurity practices.

Questions to Ask

- "Do you ask potential vendors about their cybersecurity practices?"

Including cybersecurity as an evaluation criterion helps ensure that the technology you procure is secure, much like ensuring a car has good safety features before you drive it off the lot.

Vendor Notifications

Do you require vendors to notify you of security incidents or vulnerabilities?

Next, let's discuss the importance of vendors notifying utilities of any security incidents or vulnerabilities. Think of this like safety recalls for your car. When there's a safety risk, the manufacturer sends out a notification to keep you informed and safe. Similarly, OT and IT vendors should notify utilities when they discover security incidents or vulnerabilities.

Why It's Important

Receiving timely notifications of vendor security incidents and vulnerabilities gives utilities the opportunity to prevent or respond to potential attacks. It's like getting a recall notice that allows you to fix a problem before it leads to an accident.

What to Look For

When assessing this control, verify:

- **Contractual Language:** Look for clauses in contracts that require vendors to notify the utility of any cyber incidents within a reasonable, risk-informed time frame.

Questions to Ask

- "Do your current contracts require vendors to notify you of security incidents or vulnerabilities?"
- "If not, can you include these clauses in all future procurements?"

By ensuring vendors notify you of any security issues, you can take proactive steps to protect your utility, much like addressing a car recall to keep your vehicle safe.

Contract Clauses

Do your vendor contracts include cybersecurity clauses?

Let's face it, your utility is only as strong as its weakest link, and sometimes that weak link is a third-party vendor. Imagine living in a pristine, high-security neighborhood, but your next-door neighbor leaves their doors wide open. Not great, right? That's why you need to make sure your vendors are on the same cybersecurity page as you are.

Why It's Important

Including cybersecurity clauses in vendor contracts is crucial. It ensures that your vendors are just as committed to cybersecurity as you are. This way, you're not just securing your own operations but creating a fortress that extends to everyone you work with.

What to Look For

When you're assessing this control, here's what you should be looking for:

- **Contractual Language:** Make sure every vendor contract has specific cybersecurity clauses. These should outline the vendor's responsibilities for protecting data, reporting incidents, and adhering to cybersecurity best practices.
- **Compliance Requirements:** Ensure the contracts require vendors to comply with all relevant cybersecurity regulations and standards. It's like making sure your neighbor agrees to the same HOA rules that keep the neighborhood safe.

Questions to Ask

- "Do your vendor contracts include specific cybersecurity clauses?"
- "How do you ensure vendors comply with the cybersecurity requirements outlined in their contracts?"
- "Do you review and update these clauses regularly to reflect evolving threats and regulatory changes?"

Including robust cybersecurity clauses in your vendor contracts is like having an ironclad agreement with your neighbors to keep the community secure. It ensures that everyone is doing their part to maintain a safe and protected environment.

RESPONSE AND RECOVERY

This section is about being prepared and ready to respond to and recover from a cyberattack quickly and effectively to restore and maintain operations at your utility. Imagine driving and suddenly getting a flat tire. Are you prepared? Do you have a spare tire, the necessary tools, and the know-how to fix it? Being prepared for a cyberattack is similar: it can significantly reduce downtime and help you bounce back quickly.

The key elements of response and recovery include having an incident response plan, clear reporting procedures, and cybersecurity insurance. Let's break down each element to ensure you're ready for any cyber emergency.

This Section Will Cover

28. **Incident Reporting:** Do you have a written procedure for reporting cybersecurity incidents?
29. **Incident Response Plan:** Do you have a written cybersecurity incident response plan?
30. **Backup Process:** Do you back up critical systems regularly and store backups separately from source systems?
31. **Network Topology:** Do you maintain updated documentation of your network topology?

Incident Reporting

Do you have a written procedure for reporting cybersecurity incidents?

First up, let's talk about incident reporting. Think of this as having a step-by-step guide on what to do when there's a cyber incident, much like a manual for troubleshooting your car when it breaks down.

Why It's Important

Reporting incidents to outside agencies can help a utility respond to and recover from a cybersecurity incident. The information shared can also help prevent cybercrime at other utilities by raising awareness of potential threats.

What to Look For

When assessing this control, verify:

- **Standard Operating Procedures (SOPs) and Report Templates:** Ensure there are clear procedures and templates for reporting cybersecurity incidents, distributed to all utility personnel. These can be included in the utility's emergency response plans (ERPs) or incident response plans (IRs).

Questions to Ask

- "Do you train your employees on how to follow the SOPs and report template in the event of a cyberattack?"

Having a clear and practiced incident reporting process ensures that everyone knows what to do when a cyber incident occurs, helping to minimize confusion and response time.

Incident Response Plan

Do you have a written cybersecurity incident response plan?

Next, let's discuss the incident response plan. Think back to your school days and fire drills. Everyone knew the drill: where to go, what to do. An incident response plan is your utility's fire drill for cyber incidents.

Why It's Important

An effective incident response plan outlines strategies, resources, and procedures for preparing for and responding to a cyber incident. Regularly practiced and updated, it helps ensure a quick recovery from cybersecurity incidents.

What to Look For

When assessing this control, verify:

- **Incident Response Plan Documentation:** Check that the utility has a written incident response plan, possibly integrated into their ERP, and that it's regularly practiced and updated.

Questions to Ask

- "Do you regularly practice your incident response plan by conducting drills and/or tabletop exercises?"
- "Are all staff members trained on the procedures outlined in the incident response plan?"

Practicing and updating the incident response plan ensures everyone knows their role during an incident, reducing panic and ensuring a swift, coordinated response.

Backup Process

Do you back up critical systems regularly and store backups separately from source systems?

Now, let's talk about backups. Think of this like having copies of important documents stored in a safe place. If the originals are lost or damaged, the backups ensure you can quickly restore what's necessary.

Why It's Important

Backups are crucial for restoring and recovering operations in the event of a cyber incident, hardware malfunction, or physical destruction of equipment. They are the first line of defense against ransomware attacks, allowing quick restoration without paying ransoms.

What to Look For

When assessing this control, verify:

- **Backup SOP and Schedule:** Ensure there's a clear SOP outlining the backup process and schedule, and that backups are stored separately from the source systems.

Questions to Ask

- "How often do you back up your critical systems?"
- "Where are the backups stored, and how often are they tested?"

Regular, tested backups ensure that your utility can recover critical data and systems quickly, minimizing downtime and disruption.

Network Topology

Do you maintain updated documentation of your network topology?

Lastly, let's discuss keeping your network documentation updated. Imagine your utility's OT and IT assets as a big puzzle. The documentation of network topology is the instruction manual showing how everything fits together.

Why It's Important

Network topologies are essential for diagnosing issues and identifying vulnerabilities. An up-to-date network diagram is critical for effective cyber disaster recovery.

What to Look For

When assessing this control, verify:

- **Network Topology Documentation:** Ensure there's a complete and current diagram showing all network connections and components.

Questions to Ask

- "Have you conducted a network survey to assist in developing the network topology?"
- "Do you update your topology when new OT and IT assets are introduced to the network?"

Keeping the network documentation current ensures that all new assets are accounted for and connected properly, aiding in quick identification and resolution of issues.

OTHER SECURITY MEASURES

Now, let's wrap things up with some other essential security measures. These controls are crucial but didn't quite fit within the other seven control families. We'll break down network segmentation and email security controls. Think of these as the final touches to fortify your digital home.

Network segmentation is like having doors in your house. If something goes wrong in one room, the doors prevent the threat from spreading easily to others. Email security controls act like a vigilant friend who checks your mail to ensure it's not a trick.

This Section Will Cover

32. **Network Segmentation:** Do you segment OT and IT networks and deny connections by default unless explicitly allowed?
33. **Email Security:** Do you use email security controls to reduce common email-based threats like phishing and spoofing?

Network Segmentation

Do you segment OT and IT networks and deny connections by default unless explicitly allowed?

First up, let's discuss network segmentation. Imagine your home Wi-Fi has two separate networks: one for your devices like phones and tablets and another for special gadgets like your smart thermostat and security cameras. This setup keeps your special gadgets safe, away from potential troublemakers unless you explicitly allow access.

Why It's Important

Segmentation is the practice of digitally dividing a utility's OT and IT networks. This limits the ability to access the OT network if the IT network is compromised first.

What to Look For

When assessing this control, verify:

- **Updated Network Topologies:** Ensure documentation demonstrates that OT and IT networks are segmented.

Questions to Ask

- "How do you ensure your OT and IT networks stay fully segmented?"

Segmentation helps prevent a breach in one area from spreading, much like keeping certain doors in your house locked to contain any potential threats.

Email Security

Do you use email security controls to reduce common email-based threats like phishing and spoofing?

Finally, let's address email security controls. Phishing is one of the most common methods attackers use to gain unauthorized access. While training employees to recognize phishing attempts is essential, technical controls can filter out many of these threats before they even reach your inbox.

Why It's Important

Email security controls help reduce the risk of spoofing, phishing, and email interception, protecting the network from unauthorized access.

What to Look For

When assessing this control, verify:

- **Technical Cybersecurity Controls on Email Accounts:** This information is typically found within a cybersecurity policy document.

Questions to Ask

- "Along with technical controls, do you educate your employees on how to spot common email attacks such as phishing?"

Ensuring robust email security is like having a vigilant friend who checks your mail for potential threats, helping to keep your digital home safe and secure.

What’s Next After the 33 Steps?

So, you’ve made it through all 33 steps in this guide and your utility’s cybersecurity posture is stronger than ever. You've locked the doors, checked the windows, and set up the alarms. But what’s next? This was just step one. Now you need to think about the day-to-day threats and common TTPs (tactics, techniques, and procedures) that cyber attackers might throw your way. That’s where Parsons comes in. We’re here to ensure you’re not just secure but resilient and always one step ahead of the game.

Overview of Parsons' Cybersecurity Solutions

Parsons offers a comprehensive suite of cybersecurity services designed to meet the unique needs of utilities like yours. We don’t just patch up holes; we build robust defenses that keep evolving with the threats. Here’s how we do it:

- **Full Vulnerability Assessments:** We dive deep into your equipment and network health, identifying every possible vulnerability.
- **Real-Time Cybersecurity Alerting:** Our Cyberzcape platform keeps you informed with up-to-the-second alerts about any threats.
- **Regulatory Compliance:** SigmaFlow ensures you’re always in compliance with industry regulations, making audits a breeze.

With Parsons, you get a partner who’s as committed to your security as you are. We don’t just provide solutions; we provide peace of mind.

Why Choose Parsons?

Here’s why Parsons is the perfect partner for your cybersecurity needs:

- **Proven Expertise:** We’ve got years of experience in the cybersecurity field, protecting utilities just like yours.
- **Tailored Solutions:** We provide customized solutions that address your specific needs and challenges.
- **Commitment to Excellence:** We’re committed to delivering the highest quality services and solutions.
- **Ongoing Support:** We don’t just implement solutions and walk away. We’re here to support you continuously.

Cyberzcape™
a PARSONS solution

Click here to find out more.

Cyberzcape: Comprehensive Cybersecurity Platform

Cyberzcape is the superhero of our cybersecurity arsenal. It's designed to offer you unparalleled protection across the board.

- **Threat Detection and Prevention:** Think of it as your utility's personal bodyguard, identifying and stopping threats before they can do any damage.
- **Incident Response:** When something does slip through, Cyberzcape helps you respond quickly and effectively, minimizing any impact.
- **Vulnerability Management:** We keep track of all your vulnerabilities, making sure they're patched and secure.
- **Compliance Management:** Cyberzcape also helps you stay on top of all regulatory requirements, so you're never caught off guard.

Cyberzcape isn't just a tool; it's a comprehensive solution that keeps your utility safe from every angle.

SigmaFlow™
a PARSONS solution

Click here to find out more.

SigmaFlow: Workflow Automation and Compliance Management

SigmaFlow is the unsung hero, working behind the scenes to ensure everything runs smoothly and efficiently.

- **Workflow Automation:** It streamlines your processes, reducing manual effort and increasing efficiency.
- **Compliance Tracking:** SigmaFlow keeps you in line with all regulatory requirements, ensuring your operations are always compliant.
- **Risk Management:** Identify and mitigate risks with SigmaFlow's integrated risk management tools.
- **Audit Support:** Simplify the audit process with comprehensive documentation and reporting features.

With SigmaFlow, you don't just stay compliant; you stay ahead of the curve.

So, what's the next step? Contact Parsons today to learn more about how our cybersecurity services can help you stay secure and resilient. Together, we can build a stronger, more secure future for your utility.

