Journal of Computational Analysis and Applications **VOL. 33, NO. 5, 2024**

10.48047/jocaaa.2024.33.05.33

How to Improve Cybersecurity Water and Wastewater Industries - A cost effective solution

Pankaj Kumar
Sr Project Manager, USA
Email: Pkumar@uft.com

ABSTRACT
This white paper provides a solution to improve the cybersecurity status within the water and wastewater industries. This is in continuation to the whitepaper Cybersecurity in Water and Wastewater Industries - an Eye opener published by Pankaj Kumar by examining the implementation of the National Institute of Standards and Technology (NIST) Cybersecurity Framework in three distinct organizations, referred to as Company A, Company B, and Company C (Name masked for Privacy concerns). As critical infrastructure, water and wastewater systems are increasingly targeted by cyber threats. These vulnerabilities could severely impact public health and environmental safety. This document provides a solution to these challenges and recommends strategies to strengthen security posture in alignment with NIST guidelines.

Keywords: Smart water systems

I. INTRODUCTION

In today's world, where all information systems are connected, cybersecurity becomes a necessity, particularly for organizations that have limited human expertise in cybersecurity-related skillsets and also very limited financial resources to implement a robust cybersecurity solution. This white paper uses the inputs from the study conducted by Pankaj Kumar published in the whitepaper Cybersecurity in Water and Wastewater Industries - an Eye opener and focuses on key focus areas to improve water and wastewater industries' defenses against rapidly growing cyber threats. This paper underscores the importance of spreading awareness about what cybersecurity is, how it can impact intellectual properties, disrupt businesses, Do's and Don'ts when you are operating in a potentially vulnerable environment, and how to act when such an incident occurs. This paper also reinforces the importance of sturdy identification and risk assessment and how government or industry bodies can provide additional support to safeguard the organization in case of cyber incidents. This paper also covers the critical area of Identity and access control (IAM) and segmentation, highlighting the need for strong measures like multi-factor authentication (MFA) and network partitioning to protect sensitive systems like SCADA. In this paper, the author also emphasizes the value of investing in threat detection and monitoring, discussing options such as managed detection and response services and government-backed programs. This paper also focuses on the need for an incident response plan, a reliable backup solution, and disaster recovery planning (DRP) to ensure the business can operate without interruption in case of a cyber incident. By implementing these key strategies, organizations can significantly improve their cybersecurity postures and reduce the impact of potential attacks.

Problem Statement

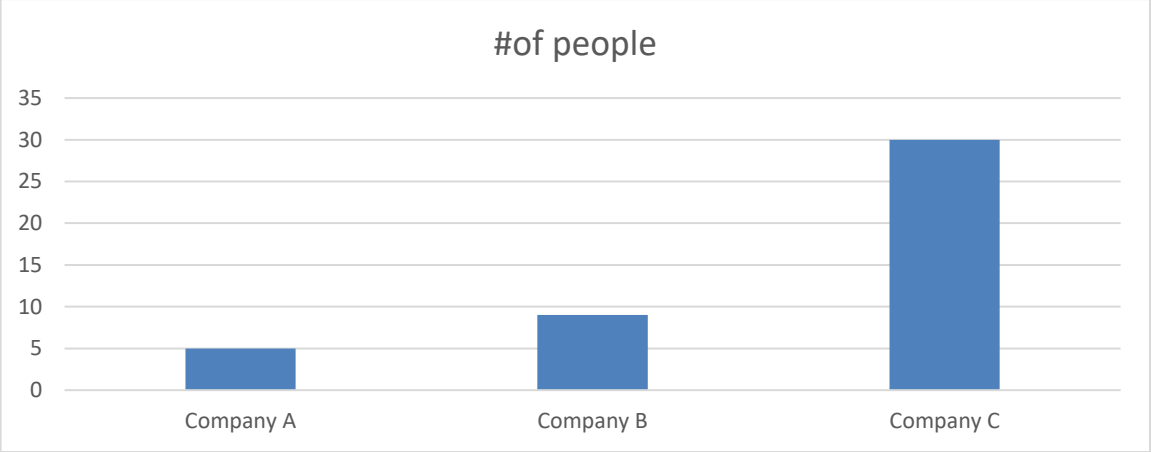
Cyber-attacks on water infrastructure can disrupt operations, compromise water quality, and pose serious health risks. Although the NIST Cybersecurity Framework offers a structured approach to managing cybersecurity risks, adoption levels vary significantly across the water and wastewater industries due to financial, technical, and personnel challenges. This white paper aims to provide solutions to some common challenges and best practices for implementing NIST-based cybersecurity measures across different organizations cost-effectively.

Methodology

This assessment is based on a comparative analysis of cybersecurity practices at three anonymous organizations:

- Company A: less than 10 member Company. Major supplier for Valves, and Chemical to the US Municipality water treatment plant, Operates in the Central part of the USA
- Company B: A mid-sized, 10 or more members company, Provider of Valve in the Central part of the USA
- Company C: A mid-sized, 15-20 employee firm, multi-site water and wastewater management company that operates in Eastern Part of the USA

10.48047/jocaaa.2024.33.05.33



Data was collected through a combination of Due diligence, employee interviews, technical assessments, and examination of each company's cybersecurity policies in relation to the NIST Cybersecurity Framework's five core functions: Identify, Protect, Detect, Respond, and Recover.

Analysis/Findings: Cybersecurity Gaps

- Limited Asset Management: Minimal control over asset management practices, especially regarding software and applications used by end-users.
- Basic Awareness of Organizational Context: Foundational understanding of business environment and dependencies but lacks depth.
- Inadequate Governance: Absence or underdevelopment of a formal governance framework for managing cybersecurity risks.
- Minimal Risk Assessment and Management: Lack of robust risk assessment processes to identify potential threats and vulnerabilities, along with inadequate mitigation strategies.
- No Formal Cybersecurity Audits: Regular cybersecurity audits are not conducted to assess security posture and identify areas for improvement.
- Basic Endpoint Protection: Insufficient to address sophisticated cyber threats.
- Inadequate Identity and Access Management: Lack of robust framework for user authentication and authorization.
- Limited Network Security: Basic or no network security controls to monitor and maintain network integrity.
- Insufficient Cybersecurity Awareness and Training: Absence or inadequacy of user training programs.
- Weak Data Protection: Limited encryption for data at rest and in transit.
- Inadequate Backup and Recovery: Basic backup procedures with no secondary solutions, increasing the risk of data loss.
- No Formal Incident Response Plan: Lack of formal plans to address and mitigate cybersecurity incidents.
- Limited Security Audits and Policy Updates: Minimal or no audits and policy reviews to identify and address vulnerabilities.
- Absence of Advanced Security Solutions: Lack of advanced technical security solutions to enhance system resilience.
- Respond: Lacks a formal incident response plan, leading to improvised responses and prolonged recovery times.
- Recover: No dedicated recovery process, resulting in prolonged downtime after cyber incidents.

Key Challenges Identified

1. **Resource Limitations**: Smaller facilities, like Company A, struggle to allocate sufficient resources for cybersecurity, impacting their ability to fully implement NIST guidelines.
2. **Skills Gap**: A shortage of specialized cybersecurity staff in all three companies hinders effective threat detection and incident response.

10.48047/jocaaa.2024.33.05.33

3. **Technology Gaps:** Older systems in water treatment facilities, especially SCADA and legacy operational technology (OT), are often incompatible with advanced security controls.
4. **Varying Levels of NIST Implementation**: Companies B and C have adopted more comprehensive NIST-aligned practices, while Company A's limitations reflect a larger industry-wide gap for smaller facilities.

Recommendations

Based on these findings, here are key recommendations for enhancing cybersecurity within water and wastewater organizations using the NIST framework in the most cost-effective ways.

1. Improving Cybersecurity Awareness in Water and Wastewater Industries: Cost-Effective Strategies

As the globe progressively depends on digital technology, the significance of cybersecurity is hard to overemphasize, particularly in vital sectors such as water and wastewater management. Cyberattacks targeting these industries can yield severe repercussions, threatening public safety and interrupting crucial services. Thus, boosting awareness and implementing economical cybersecurity strategies is essential. Here are actionable methods that organizations can employ to enhance cybersecurity awareness without overspending.

- Training and Education One of the most effective yet undervalued strategies for improving cybersecurity awareness is regular training and education for all employees. Instead of expensive seminars or workshops, companies can utilize free online resources:
- Webinars and Online Courses: Platforms like Coursera or edX offer free courses on cybersecurity fundamentals. Employees can learn at their own pace and on their own timeline.
- In-House Training Sessions: Identify a knowledgeable staff member to conduct informal training sessions. Create an environment to promote the sharing of knowledge related to cybersecurity incidents.
- Awareness Campaigns: Awareness is a preventive measure that is very effective in mitigating cyber threats by almost 80%. Organizations should promote a culture of security awareness, where they can make users aware of do's and don'ts when they are dealing with IT and OT, which can significantly mitigate risks. Low-cost awareness campaigns can be implemented by using:
- Posters and Bulletins: Create eye-catching posters that highlight key cybersecurity practices and display them in common areas. These visual reminders can help reinforce the importance of security on a daily basis.
- Monthly Newsletters: Distribute a monthly newsletter that includes the latest news in cybersecurity, practical tips, and best practices. This approach keeps the topic fresh in everyone's minds and promotes ongoing discussions.
- Simulated Phishing Exercises: Phishing is a widespread tool cybercriminals use to gain unauthorized access. An Organization can simulate phishing exercises to help employees recognize potential threats:
- Free Tools: Utilize online tools to create realistic phishing emails. Observe the results to understand how many employees clicked on the links and provide feedback accordingly. A few examples are **GoPhish** (Open Source, Free), **Phishing Frenzy** (Open Source, Free), **MailSniper** (Free, Open Source)
- Friendly Competitions: Organize friendly competitions with rewards for departments or individuals who spot the most fake phishing attempts. This encourages vigilance in a fun way.
- Collaboration and Community Engagement: Networking with other organizations can provide additional insights and learning opportunities without significant costs:
- Industry Groups: Participate in cybersecurity workshops or forums organized by industry associations. These gatherings can be invaluable for sharing knowledge and accessing resources. A few examples of such online communities are https://www.linkedin.com/groups/14488490/https://www.linkedin.com/groups/3799371/
- Community Initiatives: Partner with local government or educational institutions to host community awareness events. This not only increases awareness but also strengthens community ties. For example, https://statescoop.com/indiana-begins-offering-water-systems-free-cyber-assessments/

10.48047/jocaaa.2024.33.05.33


STATESCOOP Topics Special Reports Events Podcasts Videos Insights Sta

CYBERSECURITY

Indiana begins offering water systems free cyber assessments

Water and wastewater facilities in Indiana can now obtain free cybersecurity assessments through the state's technology office.

BY COLIN WOOD - DECEMBER 3, 2024

Listen to this article 2:51 Learn more.

Reference: Indiana Begins Offering Water Systems Free Cyber Assessments

- Policy Development: Creating and disseminating clear cybersecurity policies is essential for guiding employees' actions:
- Simple Language: Use simple language catered to audience while drafting the policies, straightforward language that everyone can understand. Emphasize on key actions required from employees.
- Regular Updates: Review and update policies periodically to reflect new threats and evolving best practices and communicate these updates via available channels to ensure everyone is informed.
- Promote a Culture of Security Hygiene Fostering a culture of security hygiene is essential for ongoing awareness:
- Encourage tool usage to securely managing Password: Advise employees to use password management tools or create strong, unique passwords. Regular reminders about changing passwords can further enhance security. For example, User should use MFA using tools like **Microsoft Authenticator, Google Authenticator, FreeOTP, or OneAuth**
- Lead by Example: Management should exemplify good cybersecurity practices. When leaders prioritize security, it sends a strong message across the organization.
- Free Cybersecurity Resources Various free resources can help organizations bolster their cybersecurity strategies:
- Federal Agencies: Websites like the Cybersecurity & Infrastructure Security Agency (CISA) offer free toolkits, training materials, and guidelines tailored to critical infrastructure sectors, including water and wastewater.
- Online Forums and Communities: Engaging with cybersecurity forums and communities can provide real-time help and advice based on current trends and challenges. Such as https://www.linkedin.com/groups/14488490/https://www.linkedin.com/groups/3799371/

There is no need to spend a lot of money raising cybersecurity awareness in the water and wastewater sectors. Organizations can greatly enhance their defenses against cyber threats by utilizing free resources and fostering a strong security culture. For example, a study discovered that businesses that provide cybersecurity training to their staff see a 50% decrease in security events. Businesses can promote a proactive approach to cybersecurity and protect critical infrastructure for the general public by devoting time and resources to training awareness campaigns and community involvement. Everyone involved in these vital services can have a safer tomorrow if awareness is raised today.

2. Enhancing Identification and Risk Assessment Capabilities in Water and Wastewater Systems through Cost-Effective Cybersecurity Measures

In order to increase efficiency and service delivery in the increasingly interconnected world of today, water and wastewater systems are utilizing advanced technologies. New difficulties, especially in the field of cybersecurity, accompany these developments, though. Protecting these vital infrastructures is crucial for health and safety of people as well as operational effectiveness. With a focus on cybersecurity, we examine practical and reasonably priced methods to improve these systems capacity for identification and risk assessment.

- Knowing the Cyber Threat Landscape: Recognizing the possible cyber threats that water and wastewater systems may encounter is the first step towards improving risk assessment. Common weaknesses could be malware attacks phishing schemes directed at staff members and illegal access to control systems. To lay a solid basis for defensible infrastructure a comprehensive evaluation of potential risks must be carried out.

10.48047/jocaaa.2024.33.05.33

- Utilizing Existing Resources: Internal data including service records incident reports and maintenance logs are already in the possession of many organizations. Systems can find trends of previous security lapses or system failures by carefully examining this data. Without requiring a large financial outlay this analysis can assist in identifying weak points and areas that need urgent attention.
- Programs for employee awareness and training: In cybersecurity people are frequently the weakest link. Organize frequent training sessions to inform staff members about typical cyberthreats and security procedures. Organizations can greatly lower the risk of breaches by encouraging awareness of how to spot phishing emails or social engineering techniques.
- Internal training initiatives that emphasize creating a security-conscious culture among employees can be created at a comparatively low cost.
- Establishing cooperative relationships with nearby academic establishments can provide important information about cybersecurity risks and defenses. Fresh viewpoints and possibly affordable solutions can be offered by cybersecurity researchers and students. In addition to allowing students to obtain real-world experience, internships and group projects can encourage creativity.
- Adopting low-cost security technologies is important, but they don't have to be expensive. Examples include intrusion detection systems, firewalls, and encryption tools. Numerous open-source programs offer strong security features at affordable prices. Additionally, without incurring large costs, multi-factor authentication (MFA) for access controls can greatly improve security.
- Conducting routine cybersecurity audits can help identify weaknesses and guarantee adherence to industry norms. These audits can be performed out internally or in collaboration with cybersecurity professionals who are prepared to provide pro bono services as part of community outreach. Frequent evaluations foster proactive risk management and a culture of continuous improvement.
- The creation of an incident response plan is essential to reducing the harm caused by a cyberattack. To ensure employees are ready to manage cyber incidents effectively, organizations should regularly test their cyber threat response protocols. This includes clearly stating lines of communication and assigning specific responsibilities to team members in the event of a cyber threat or cyber incident.

Involving the Community: Promoting participation from the local community can also help identify risks. Residents can serve as the water system's eyes and ears by reporting anomalies or questionable activity that might point to a possible security risk. Overall, security can be strengthened by fostering a sense of shared responsibility and trust. To safeguard our communities from cyber threats, it is essential to improve the identification and risk assessment capabilities of water and wastewater systems. By utilizing current resources, raising employee awareness, collaborating with nearby institutions, and implementing affordable technologies, businesses can greatly strengthen their cybersecurity posture without having to pay exorbitant costs. By working together to strengthen these systems, we can safeguard vital infrastructure while simultaneously improving public health and safety and building a more resilient future for everybody.

3. Strengthen Access Control and Segmentation

Organizations confront numerous cyber threats in today's digital environment, which can have serious financial repercussions. To counter these threats, network segmentation and access control can be strengthened. It is crucial to put strong access controls in place; for instance, using Multi-Factor Authentication (MFA) for all remote access points greatly improves security. This extra security measure guarantees that unauthorized users will find it difficult to access sensitive systems even in the event that a password is compromised. Additionally, by separating vital systems from less secure networks, network segmentation is essential for protecting them. Teams can effectively contain breaches and lessen their impact on the infrastructure as a whole by segmenting the network to limit the potential spread of an attack. In addition to improving security, these tactics can result in significant financial savings. Organizations can more effectively use their resources by preventing breaches and lowering the chance of expensive data loss or fines from the government. Additionally, keeping a strong security posture lowers the possibility of expensive downtime brought on by cyber incidents. Purchasing these security measures is a proactive way to safeguard priceless assets and guarantee business continuity, not just for compliance purposes. An essential component of any affordable cybersecurity strategy will continue to be the adaptation of network segmentation techniques and access controls as cyber threats change. By making these steps a top priority, companies can build a strong security framework that reduces risks and maximizes operational effectiveness, protecting their bottom line from the constantly evolving cyberthreat landscape.

An organization can improve segmentation and access control by using these free tools.

10.48047/jocaaa.2024.33.05.33

- **Multi-Factor Authentication (MFA).**
- A straightforward smartphone app for two-factor authentication is called Google Authenticator.
- Authy: Provides backup options for 2FA and an easy-to-use interface.
- The free tier services for MFA deployment are offered by Duo Security.
- A free program for managing two-factor authentication with Microsoft accounts and other things is called Microsoft Authenticator.
- **Regarding network segmentation:**
- Segmented networks can be established with the aid of pfSense, an open-source firewall/router program.
- Another open-source firewall with management and network segmentation tools is OPNsense.
- VLAN Setup on Managed Switches: Many managed switches offer free VLAN setup options for network segmentation.
- **Regarding Access Control:**
- A free implementation of the Lightweight Directory Access Protocol for access control and directory services is called OpenLDAP.
- An open-source RADIUS server for network authentication is called FreeRADIUS.
- OpenWeakness (OWASP): OWASP offers methods and guidelines for implementing secure access control, but it is not a tool.
- **Awareness of general security.**
- Security Onion: An open-source free Linux distribution for network security monitoring and intrusion detection.
- Nmap: A free network scanning program that can assist in determining the devices on your network and evaluating network segmentation. Your security posture can be greatly improved with these reasonably priced tools.

4. Invest in Threat Detection and Monitoring

Threat detection and monitoring entails locating and evaluating possible security risks to the networks and information systems of an organization. To identify indicators of compromise (IOCs), such as anomalous network traffic or unauthorized access attempts, this procedure involves ongoing surveillance using a variety of security tools. To promptly identify threats, automated systems such as intrusion detection systems (IDS) and security information and event management (SIEM) solutions are essential for examining logs and alerts. Monitoring is the process of continuously observing networks and systems to make sure they are operating safely and correctly. This entails monitoring performance indicators, incident response efforts, and system health. A strong cybersecurity strategy requires both threat detection and monitoring since they give organizations the visibility they need to recognize and reduce risks before they become serious incidents.

Investing in these areas encourages a proactive approach to information security maintenance and helps organizations remain alert to changing cyber threats. For businesses that might not have the funds to support an internal team, investing in threat detection and monitoring is essential to preserving cybersecurity.

- Companies can benefit from professional analysis and quick response with **Managed Detection and Response (MDR) services**, which eliminate the need for substantial internal infrastructure.
- As an alternative, **a number of free tools can improve threat detection and monitoring** efforts for those with limited funds.
- For example. Essential tools for intrusion detection, network security monitoring, and log management are included in the open-source Security Onion Linux distribution.
- An open-source host-based intrusion detection system (HIDS) called OSSEC is another well-liked tool that keeps an eye on process file integrity and logs for unusual activity.
- The open-source Snort program can also be used as a network intrusion detection system assisting with traffic analysis and real-time threat blocking.
- Organizations can more easily detect anomalies by using the Elastic Stack, which consists of Elasticsearch Logstash and Kibana to efficiently ingest, analyze, and visualize log data. Putting these tools into practice can improve an organization's security posture by guaranteeing that possible threats are identified and dealt with quickly.

Even though free tools have a lot of functionality, it's crucial to think about how to integrate and manage these systems within the organization's larger cybersecurity plan. Businesses may successfully improve their threat detection skills by combining free and paid services, enabling them to proactively manage risks and safeguard important assets in the increasingly complicated cyber environment of today. In the end, this combination of

10.48047/jocaaa.2024.33.05.33

resources can help create a safer online environment by enabling even smaller facilities to maintain a high level of security without going over their operating budgets.

5. Formalize and Regularly Update Incident Response Plans

Organizations of all sizes must implement strong cybersecurity measures due to the growing frequency and complexity of cyber threats. The establishment and frequent revision of incident response plans (IRPs) are essential components of a successful cybersecurity strategy. Organizations must create a thorough incident response plan in order to handle possible security incidents. These plans should follow established guidelines like those from the National Institute of Standards and Technology (NIST) and should include instructions on what to do in the event of a cyberattack. Organizations can protect their assets and data integrity using NIST's framework, which offers an organized method for anticipating, responding to, and recovering from cybersecurity incidents. For these plans to remain effective, organizations must regularly perform tabletop drills and exercises. By allowing team members to rehearse their roles in an incident response scenario, these simulations help to improve departmental coordination and foster a clear understanding of protocols. These exercises also offer great chances to find any holes in current plans and make adjustments in real time based on lessons learned.

6. Companies can support these efforts by using affordable tools like Google Workspace or Microsoft Teams for team planning and communication during exercises.
7. Tools like Asana or Trello can be used to manage tasks and responsibilities for incident tracking and documentation without breaking the bank.
8. Additionally, tools such as **GitHub** can be used as a platform for exchanging and managing versions of incident response plan documents. Organizations must keep their IRPs updated on a regular basis to stay on top of the ever-changing threat landscape. New vulnerabilities are frequently found, and cyber threats are ever evolving. Organizations can react to incidents quickly and efficiently by keeping the incident response plan up to date, which guarantees that it reflects the most recent intelligence and industry best practices. To sum up, cybersecurity is a critical issue for all businesses. Through the implementation of cost-effective tools, regular training, and the formalization and updating of incident response plans, organizations can improve their readiness. By being proactive, this strategy reduces the impact of possible incidents and cultivates a security-aware culture throughout the entire company.

9. Focus on Recovery and Resilience

In today's digital environment, cybersecurity is essential to preventing organizations' vital information from falling into the wrong hands or becoming inaccessible and to ensuring that businesses can continue to run efficiently. The significance of resilience and recovery is a crucial element that is frequently disregarded. Not only must organizations prevent cyber incidents, but they also need to be ready to implement their incident response plan when they do happen. Businesses can drastically reduce downtime and data loss following a breach by putting disaster recovery plans, data restoration procedures, and trustworthy offline backups in place. These measures need to be consistently updated to make sure they work as intended. It is crucial to keep backups up to date with the most recent data and to store them securely offline, ensuring availability in case of internet threats. A thorough disaster recovery plan should also be created and documented by organizations to aid in a speedy recovery.

There are several open-source and free tools that can help businesses improve their cybersecurity without spending a lot of money. These are some suggestions.

- Clonezilla: Perfect for offline data storage and restoration, this free open-source disk imaging tool makes it simple for users to clone hard drives and make backups.
- Comodo Backup: This free backup service ensures that regular backups are created and that data is readily accessible by integrating with storage options such as cloud storage and personal computers.
- Duplicati: This free backup solution is specifically made for online backups. To protect data, it provides file encryption and compression and supports a variety of cloud storage services.
- TestDisk is a robust open-source tool that aids in the recovery of erased partitions and the restoration of disk bootability in the event of data loss or corruption.

By using these tools and focusing on recovery and resilience, organizations can improve their cybersecurity signature and be prepared for potential threats. This proactive strategy increases the organization's overall resilience, in addition to safeguarding data.

Conclusion

Given their direct influence on environmental protection public safety and health the significance of cybersecurity

10.48047/jocaaa.2024.33.05.33

in the water and wastewater sectors cannot be emphasized. This paper emphasizes how notable cybersecurity gaps are caused by smaller utilities frequent struggles with resources and expertise. Their resistance to cyberattacks can be significantly increased though by implementing economical tactics that are in line with the NIST Cybersecurity Framework. Businesses of all sizes in water and waster water industries can significantly improve their security posture by utilizing free resources cultivating a proactive security culture and focusing on crucial areas like threat detection segmentation identity management access control and effective incident response planning. By doing this the water and wastewater sectors will ensure long-term dependability and confidence in crucial community services while simultaneously protecting their critical infrastructure public health and environmental safety.

References

1. National Institute of Standards and Technology (NIST). (2018). "Framework for Improving Critical Infrastructure Cybersecurity."
2. Cybersecurity and Infrastructure Security Agency (CISA). "Cybersecurity Best Practices for Industrial Control Systems in Critical Infrastructure."
3. Water Information Sharing and Analysis Center (WaterISAC). “Cybersecurity Threats and Mitigations in the Water Sector.”
4. S., V., Khonimkulov, A., & R., E. (2023). Data Privacy and Security in Cloud Computing Environments. E3S Web of Conferences. https://doi.org/10.1051/e3sconf/202339904040
5. Cybersecurity to Protect Dams & Critical Infrastructure - LHWP. https://www.lhwp.org.ls/cybersecurity-to-protect-dams-critical-infrastructure/
6. https://statescoop.com/indiana-begins-offering-water-systems-free-cyber-assessments/
7. https://www.linkedin.com/groups/14488490/
8. https://www.linkedin.com/groups/3799371/

Credits

1. Sonny Garcia – Network and Security Architect, UFT for his outstanding support in data collection, review, and Feedback
2. Navin Chandra – CIO of UFT, for his recommendations