10.48047/jocaaa.2022.30.02.28

Cybersecurity in Water and Wastewater Industries - an Eye opener

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

ABSTRACT
This white paper assesses the cybersecurity status within the water and wastewater sectors 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, exposing vulnerabilities that could impact public health and environmental safety. This document provides a data-driven analysis of these challenges and recommends strategies to strengthen security posture in alignment with NIST guidelines.

Keywords: Water Treatment Facilities

I. INTRODUCTION

As we become more and more dependent on digital systems in water and wastewater treatment facilities, the industry faces exponentially increased cyber threats, particularly ransomware, threats from insiders, and state-sponsored attacks. This sector's vulnerabilities to cyberthreats could lead to severe public health and environmental issues and has a damaging impacts on US critical infrastructure if not addressed effectively. This paper focuses on evaluating the current cybersecurity frameworks of three service/equipment provider firms within this sector and evaluates their adoption of NIST guidelines to identify gaps and suggest improvements.

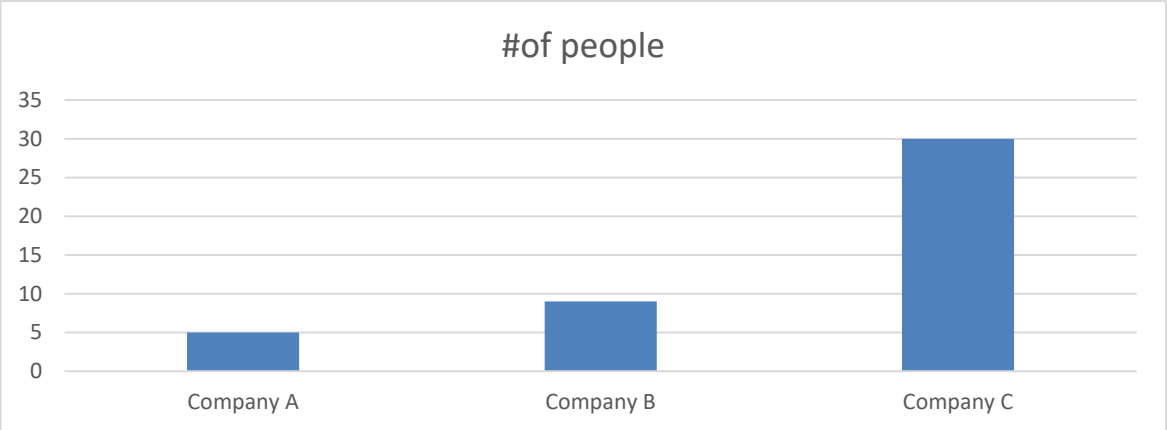
Problem Statement

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 identify common challenges and best practices in implementing NIST-based cybersecurity measures across different organizations.

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



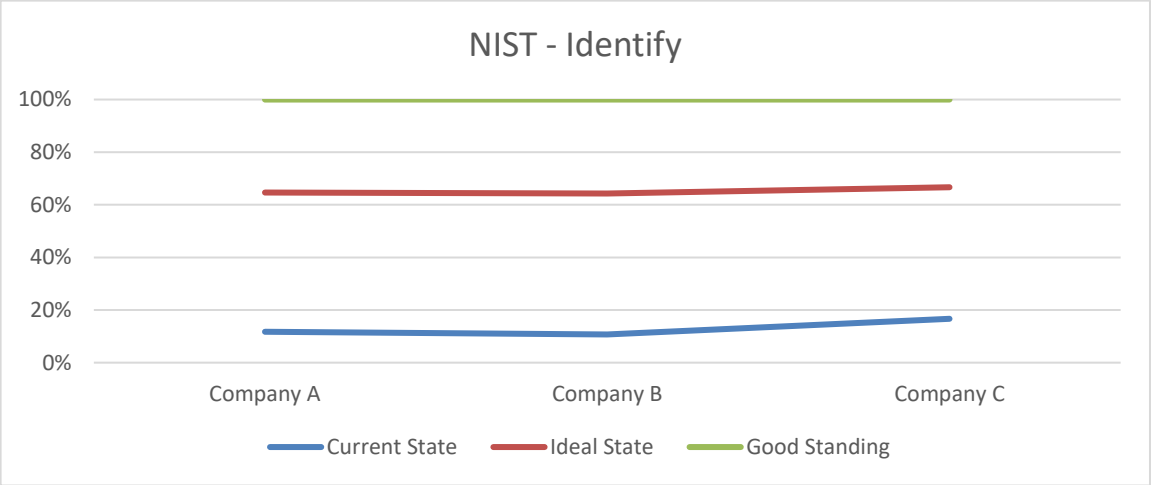
Data was collected through a combination of Due diligence, employee interviews, technical assessments, and examination of each company's cybersecurity policies in relation to the NIST Cybersecurity Framework's five core

10.48047/jocaaa.2022.30.02.28

functions: Identify, Protect, Detect, Respond, and Recover.

Analysis/Findings

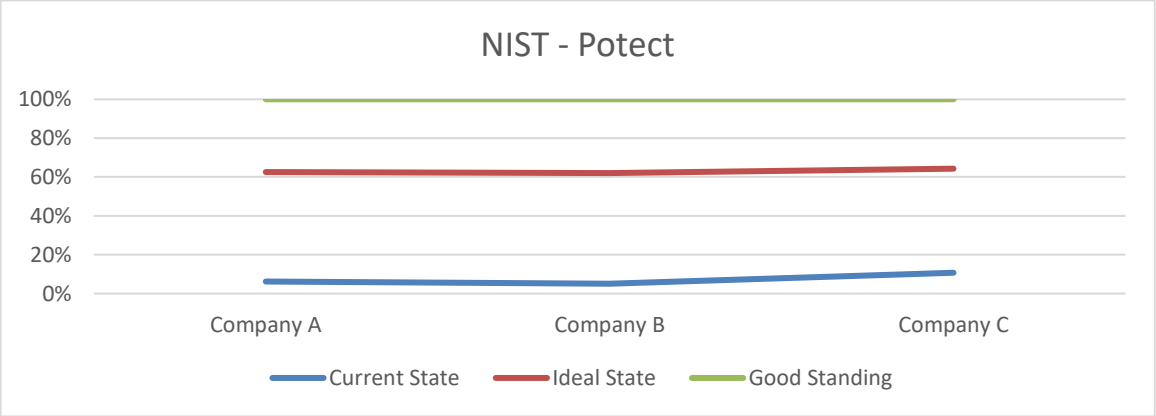
1. Identify: It focuses on developing an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. There are sets of questionnaires that help in gathering this information provided in appendix section of this white paper.



Conclusion: Based on our analysis of the data for these 3 companies, these companies have:

- Limited Asset Management: The organization exhibits minimal control over its asset management practices, particularly regarding software and applications utilized by end-users.
- Basic Awareness of Organizational Context: The organization possesses a foundational understanding of its business environment, supply chain, critical infrastructure, and organizational dependencies.
- Inadequate Governance: A formal governance framework for managing cybersecurity risks is either absent or underdeveloped.
- Minimal Risk Assessment and Management: The organization lacks a robust risk assessment process to identify potential threats and vulnerabilities, assess their potential impact, and implement effective mitigation strategies. Risk management strategies, including mechanisms for tracking, managing, and mitigating risks, are largely absent.
- No Formal Cybersecurity Audits: The organization does not conduct regular cybersecurity audits to assess its current security posture, risk management strategy, and identify areas for improvement.

2. Protect: It focuses on developing and implementing appropriate safeguards to ensure the delivery of critical services

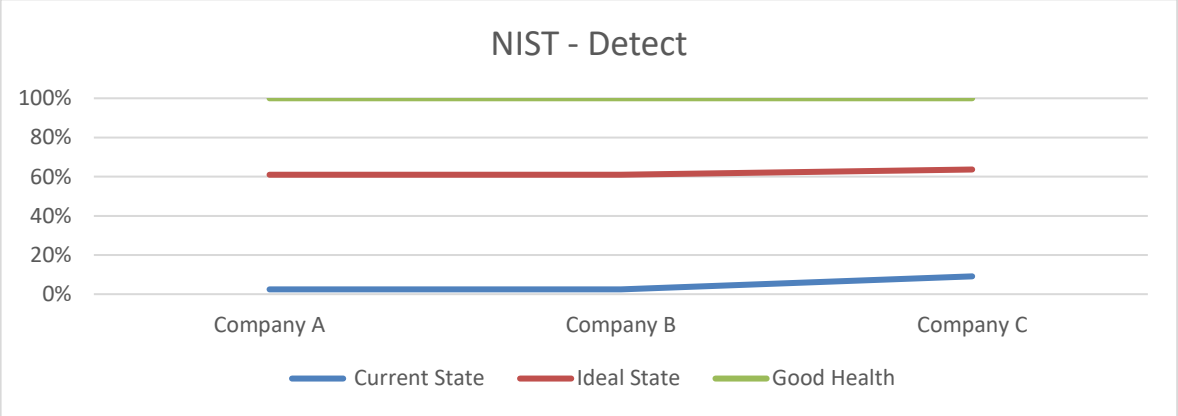


10.48047/jocaaa.2022.30.02.28

Conclusion: Based on our analysis of the data for these 3 companies, these companies have:

- Basic Endpoint Protection: While basic endpoint protection is in place, it may not be sufficient to address sophisticated cyber threats.
- Inadequate Identity and Access Management: The organization lacks a robust identity and access management framework, resulting in insufficient control over user authentication and authorization.
- Limited Network Security: The organization has basic or no network security controls in place to monitor and maintain network integrity and availability.
- Insufficient Cybersecurity Awareness and Training: Cybersecurity awareness and training programs for users are either absent or inadequate.
- Weak Data Protection: The organization has limited data protection measures, with insufficient encryption for data at rest and in transit.
- Inadequate Backup and Recovery: Backup procedures are basic, and secondary backup solutions are absent, increasing the risk of data loss.
- No Formal Incident Response Plan: Two out of three companies lack a formal incident response plan to effectively address and mitigate cybersecurity incidents.
- Limited Security Audits and Policy Updates: The organization conducts minimal or no security audits and policy reviews, hindering the ability to identify and address security vulnerabilities.
- Absence of Advanced Security Solutions: The organization does not implement advanced technical security solutions to enhance the security and resilience of its systems and assets.

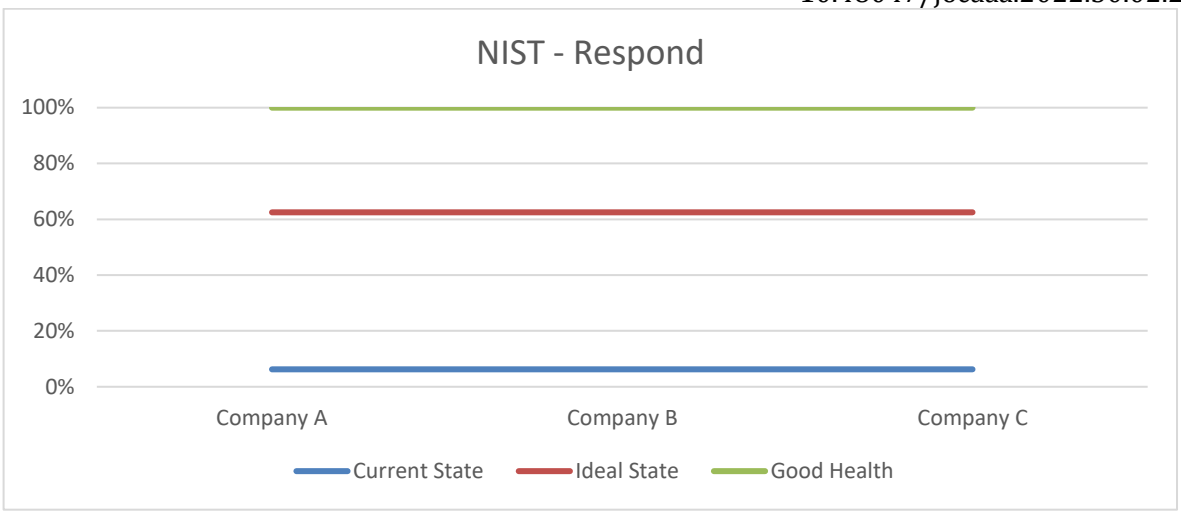
3. Detect**:** It focuses on developing and implementing appropriate activities to identify the occurrence of a cybersecurity event.



Conclusion: Based on our analysis of the data for these 3 companies, these companies have:

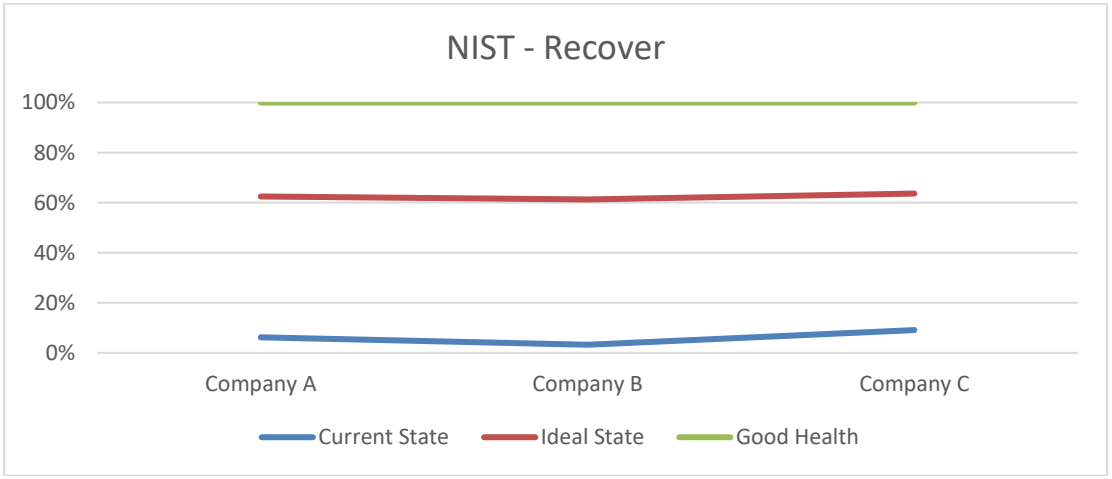
4. Respond**:** Lacks a formal incident response plan; response is often improvised, impacting recovery time.

10.48047/jocaaa.2022.30.02.28



Conclusion:

5. **Recover:** No dedicated recovery process for cyber incidents, leading to prolonged downtime after attacks.



Conclusion:

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.
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:

1. Enhance Identification and Risk Assessment Capabilities

- Implement regular asset management and vulnerability assessments, particularly for companies with limited resources. Partnering with government or industry bodies for grants or resources can support these assessments.

10.48047/jocaaa.2022.30.02.28

2. Strengthen Access Control and Segmentation

- Implement strong access controls, such as MFA for all remote access points, and ensure network segmentation to isolate critical systems from less secure networks.

3. Invest in Threat Detection and Monitoring

- Consider managed detection and response (MDR) services or government-supported cybersecurity monitoring programs for facilities unable to maintain in-house cybersecurity teams.

4. Formalize and Regularly Update Incident Response Plans

- Develop and test incident response plans that align with NIST's guidelines. Conduct regular tabletop exercises and drills to ensure all employees are prepared.

5. Focus on Recovery and Resilience

- Implement and regularly test offline backups, data restoration processes, and disaster recovery plans to minimize downtime and data loss after a cyber-incident.

Conclusion

The water and wastewater industries play an essential role in public safety, making cybersecurity a critical priority. This white paper's analysis of Company A, Company B, and Company C shows that while larger companies have implemented more comprehensive security measures, smaller utilities face significant resource challenges. By prioritizing a NIST-aligned approach and utilizing available federal and state resources, all water and wastewater facilities can improve their cybersecurity resilience.

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."

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

This white paper provides a factual assessment of the current cybersecurity status in the water and wastewater sector, highlights key challenges, and offers actionable recommendations based on NIST's proven framework. By adopting these measures, water and wastewater companies can build stronger defenses against cyber threats, ensuring the safety and reliability of critical infrastructure systems.