ARCHER

Cyber Security

Securing your digital world

The Urgent Need

Cybersecurity in Water Systems

1/ IRANIAN GOVERNMENT HACKERS ATTACKED U.S. UTILITIES, INCLUDING WATER SYSTEMS

- *Exploited Unitronics programmable logic controllers (PLCs)*
- *November 2023*
- https://www.cisa.gov/news-events/alerts/2023/11/28/exploitation-unitronics-plcs-used-water-and-wastewater-systems

2/ CHINA'S VOLT TYPHOON GROUP HACKED INFRASTRUCTURE SYSTEMS AND DRINKING WATER FACILITIES IN THE US

- *Aim to disrupt OT assets via IT networks*
- *February 2024*
- https://www.cisa.gov/sites/default/files/2024-02/aa24-038a-jcsa-prc-state-sponsored-actors-compromise-us-critical-infrastructure_1.pdf

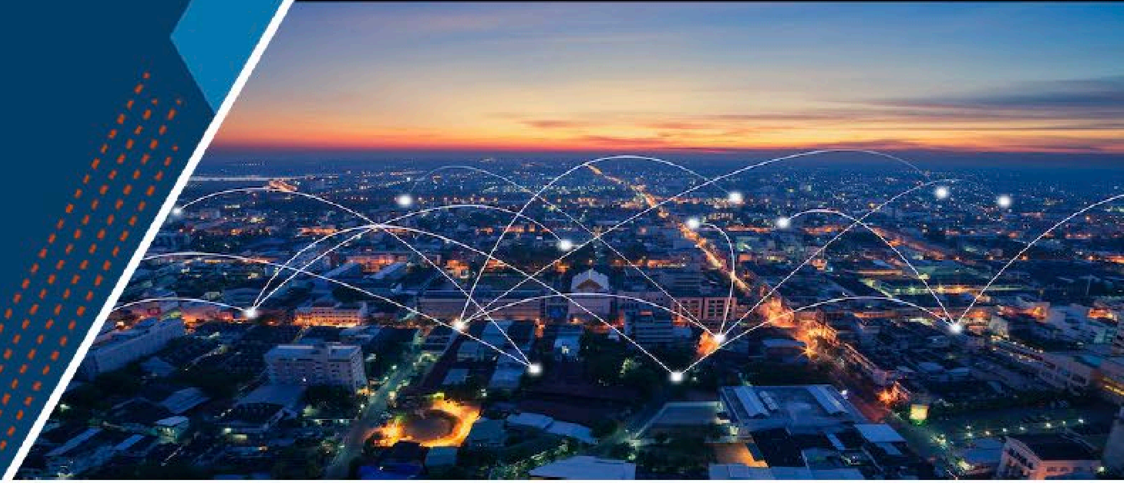
3/ INCREASINGLY SOPHISTICATED THREATS AGAINST INDUSTRIAL CONTROL SYSTEMS

- *As threats get more complex, there is a need for highly skilled technologists to match.*
- *Security tools are only part of the solutions, aware and qualified people are essential.*

4/ MORE CONNECTIVITY + INCREASED COMPLEXITY = ELEVATED SECURITY RISK

- *The devil to security is complexity*
- *Ransomware more effective*

Defending OT Operations Against Ongoing Pro-Russia Hacktivist Activity



USDA

FDA U.S. FOOD & DRUG ADMINISTRATION

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

Communications Security Establishment
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

National Cyber Security Centre
a part of GCHQ

Overview

The Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), National Security Agency (NSA), Environmental Protection Agency (EPA), Department of Energy (DOE),

Actions to take today:

- Immediately change all default passwords of OT devices

Cyber Threats and Vulnerabilities

Operational Technology (OT) systems embody a vulnerability nexus, where aging infrastructure, expanding connectivity, and the tightrope walk between open access and robust security converge.

1/ OUTDATED LEGACY TECHNOLOGY

OT systems commonly use obsolete tech that is increasingly vulnerable to cyberattacks.

2/ INCREASING INTERCONNECTIVITY

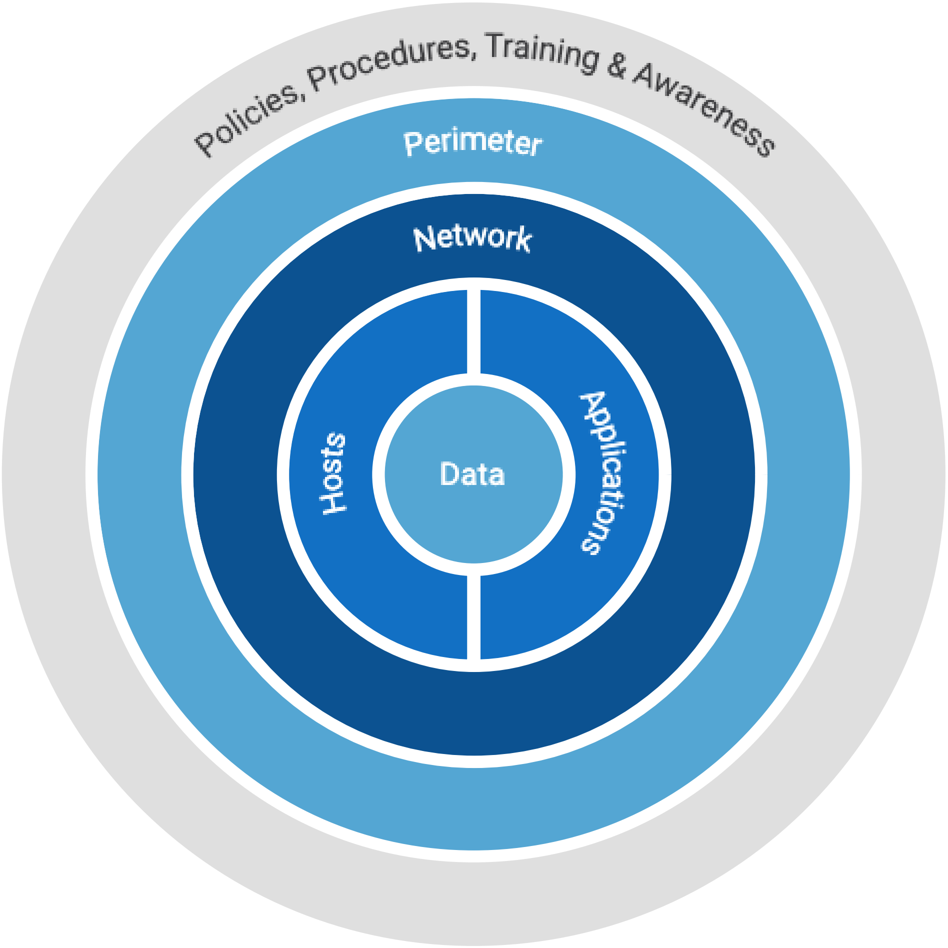
The need for more data results in increased connections, multiplying the attack surface.

3/ CONFLICTING NEEDS

Accessibility and security measures can clash, creating vulnerabilities in attempts to balance the two.

Understand Risk & Strengthening Defenses

Getting ahead of the game before mandatory and enforceable standards are forced upon us



Incident Response

A key factor in industrial control system resilience

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY -
Cyber Security
Incident
Response
Plan

Recovery and Building Resilience

Recovery is not just about restoring systems, but also about learning and improving from the experience

RESTORATION AND RECOVERY OPERATIONS

CONDUCTING TESTING EXERCISES AND TECHNICAL ANALYSIS

REVIEW AND UPDATE INCIDENT RESPONSE PLANS

Leveraging Resources

Build cybersecurity programs using best of breed methods.

EPA

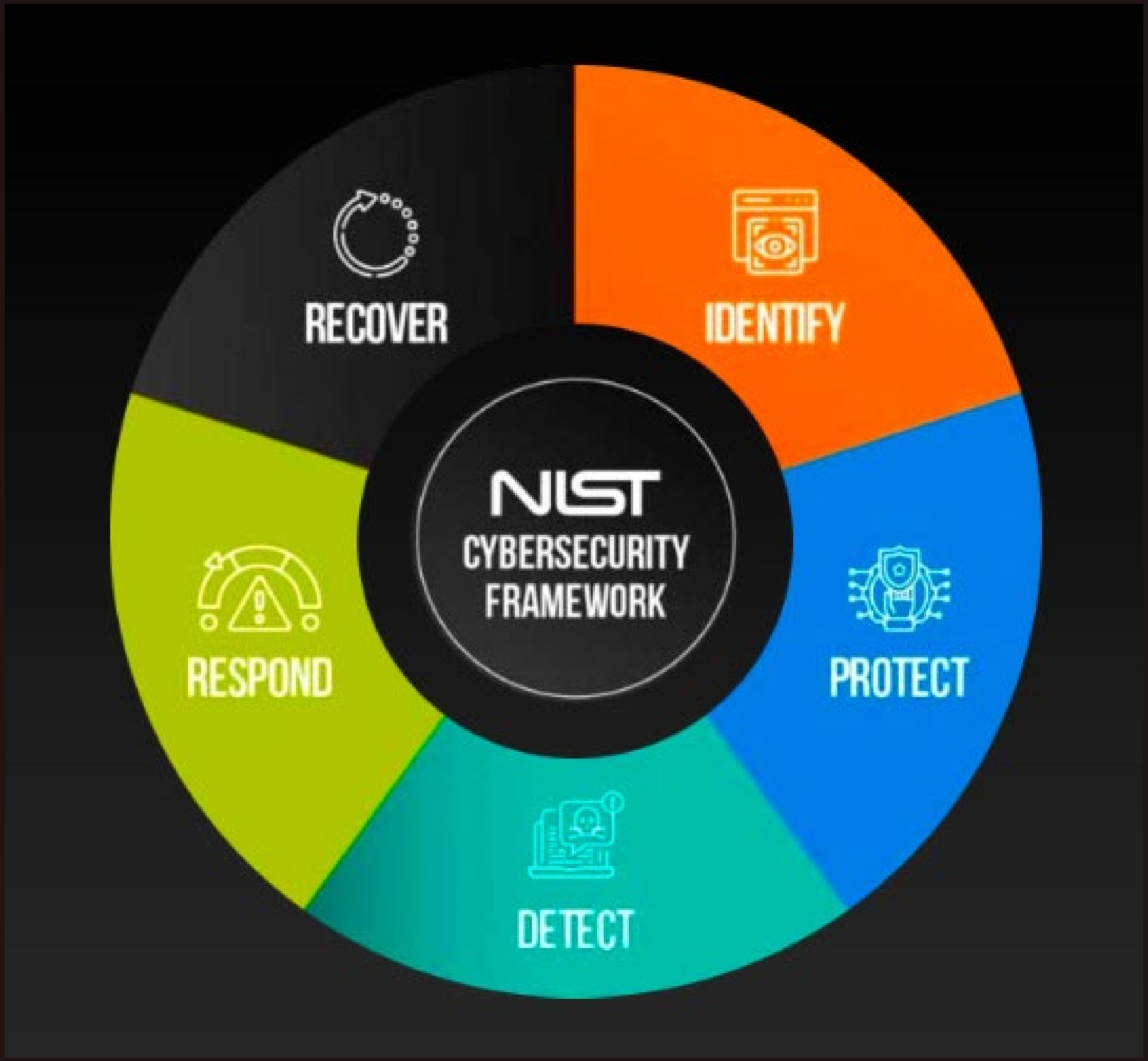
Industry specific guidance and tools

DHS

Critical Infrastructure support

NIST

Cybersecurity Framework



Conclusion

Continuous improvement is the cyber security game

- THREATS TO INDUSTRY ARE REAL
- AS CONNECTIVITY INCREASES, SO DO SECURITY RISKS
- CYBER SECURITY IS A BUSINESS ENABLER
- USE AVAILABLE RESOURCES
- EDUCATE YOUR TECHNOLOGISTS