INL/EXP-24-80778-Revision-0

Cyber-Informed Engineering Water Booster Pump Station Case Study Slides

September 2024

Benjamin Ruhlig Lampe, Virginia L Wright

Changing the World's Energy Future

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/EXP-24-80778-Revision-0

Cyber-Informed Engineering Water Booster Pump Station Case Study Slides

Benjamin Ruhlig Lampe, Virginia L Wright

September 2024

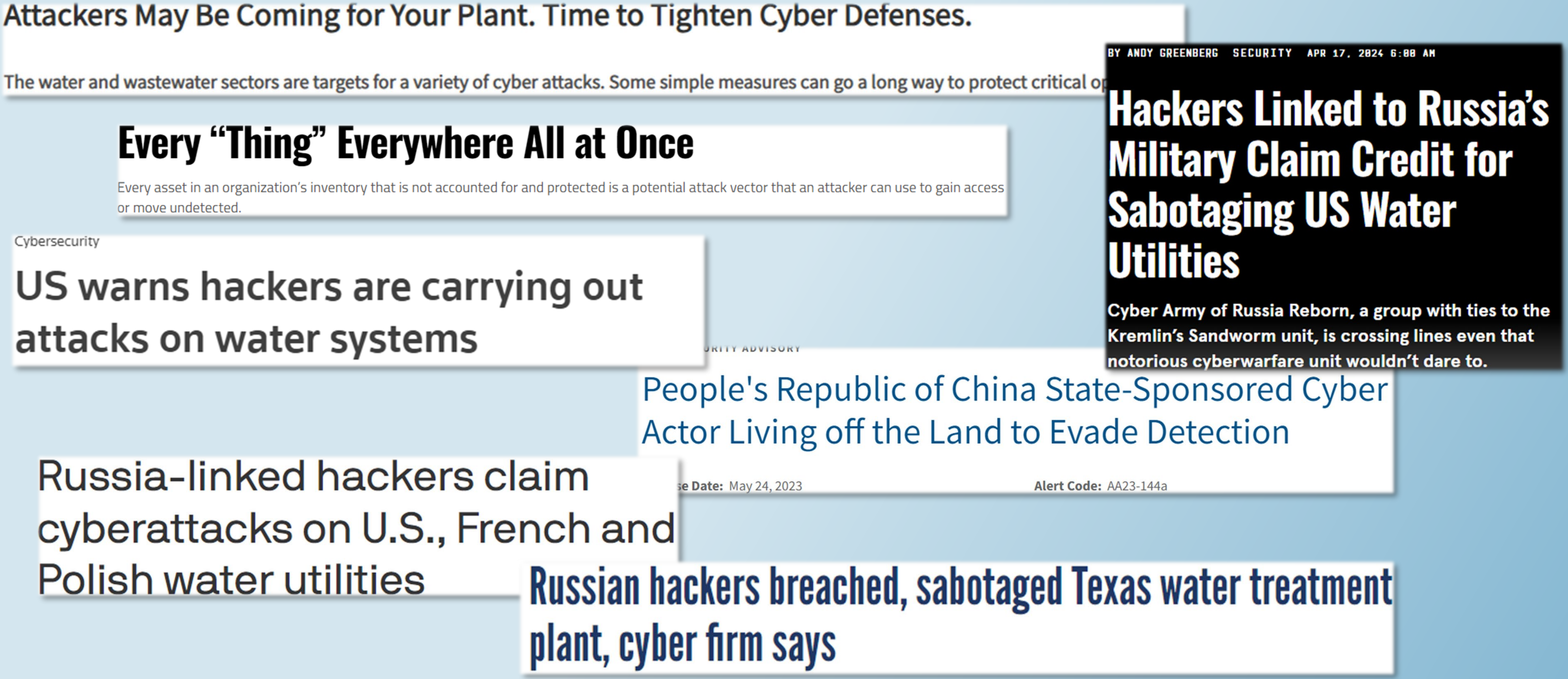
Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Cyber-Informed Engineering

Cybersecurity Threats are no longer Just Theoretical



Attackers May Be Coming for Your Plant. Time to Tighten Cyber Defenses.

The water and wastewater sectors are targets for a variety of cyber attacks. Some simple measures can go a long way to protect critical op

BY ANDY GREENBERG SECURITY APR 17, 2024 6:00 AM

Hackers Linked to Russia's Military Claim Credit for Sabotaging US Water Utilities

Cyber Army of Russia Reborn, a group with ties to the Kremlin's Sandworm unit, is crossing lines even that notorious cyberwarfare unit wouldn't dare to.

Every "Thing" Everywhere All at Once

Every asset in an organization's inventory that is not accounted for and protected is a potential attack vector that an attacker can use to gain access or move undetected.

Cybersecurity

US warns hackers are carrying out attacks on water systems

URITY ADVISORY

People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection

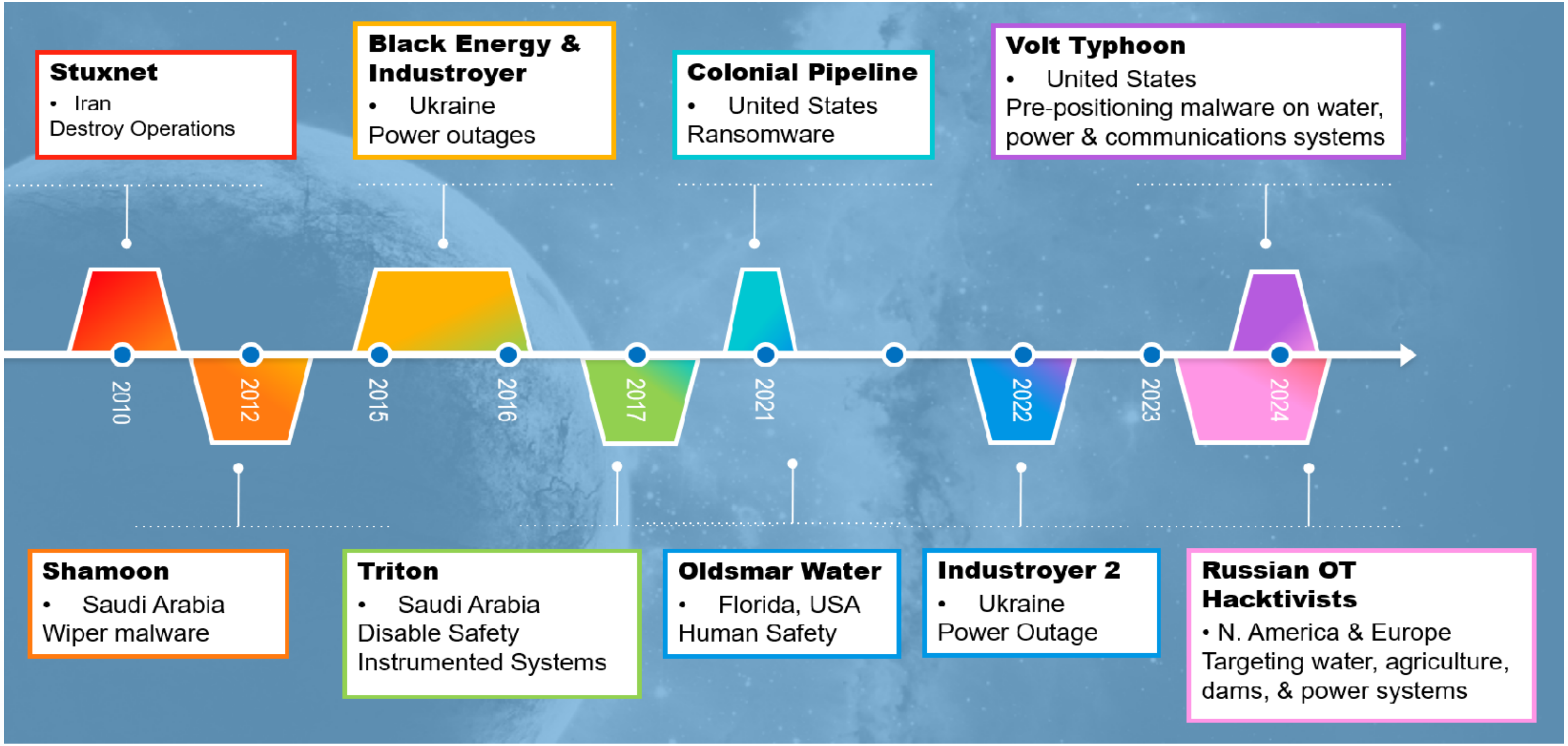
se Date: May 24, 2023

Alert Code: AA23-144a

Russia-linked hackers claim cyberattacks on U.S., French and Polish water utilities

Russian hackers breached, sabotaged Texas water treatment plant, cyber firm says

Cyber Attacks on Control Systems are Real – and Growing



Stuxnet
- Iran

Destroy Operations

Shamoon
- Saudi Arabia

Wiper malware

Black Energy & Industroyer
- Ukraine

Power outages

Triton
- Saudi Arabia

Disable Safety Instrumented Systems

Colonial Pipeline
- United States

Ransomware

Oldsmar Water
- Florida, USA

Human Safety

Industroyer 2
- Ukraine

Power Outage

Volt Typhoon
- United States

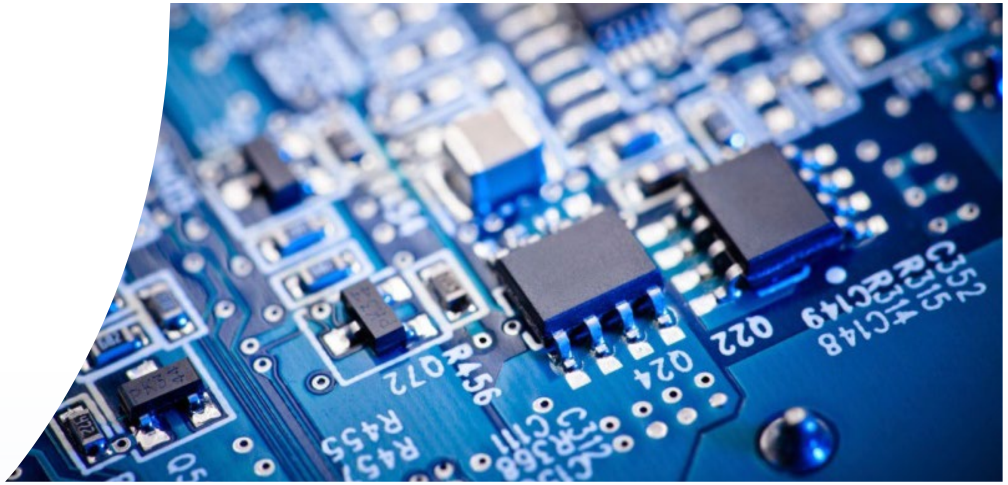
Pre-positioning malware on water, power & communications systems

Russian OT Hacktivists
- N. America & Europe

Targeting water, agriculture, dams, & power systems

Cyber-Informed Engineering (CIE)

- CIE uses **design decisions and engineering controls** to eliminate or mitigate avenues for cyber-enabled attack.
- CIE offers the **opportunity to use engineering to eliminate specific harmful consequences** throughout the design and operation lifecycle, rather than add cybersecurity controls after the fact.
- Focused on **engineers and technicians**, CIE provides a framework for cyber education, awareness, and accountability.
- CIE aims to create a **culture of security** aligned with the existing industry safety culture.



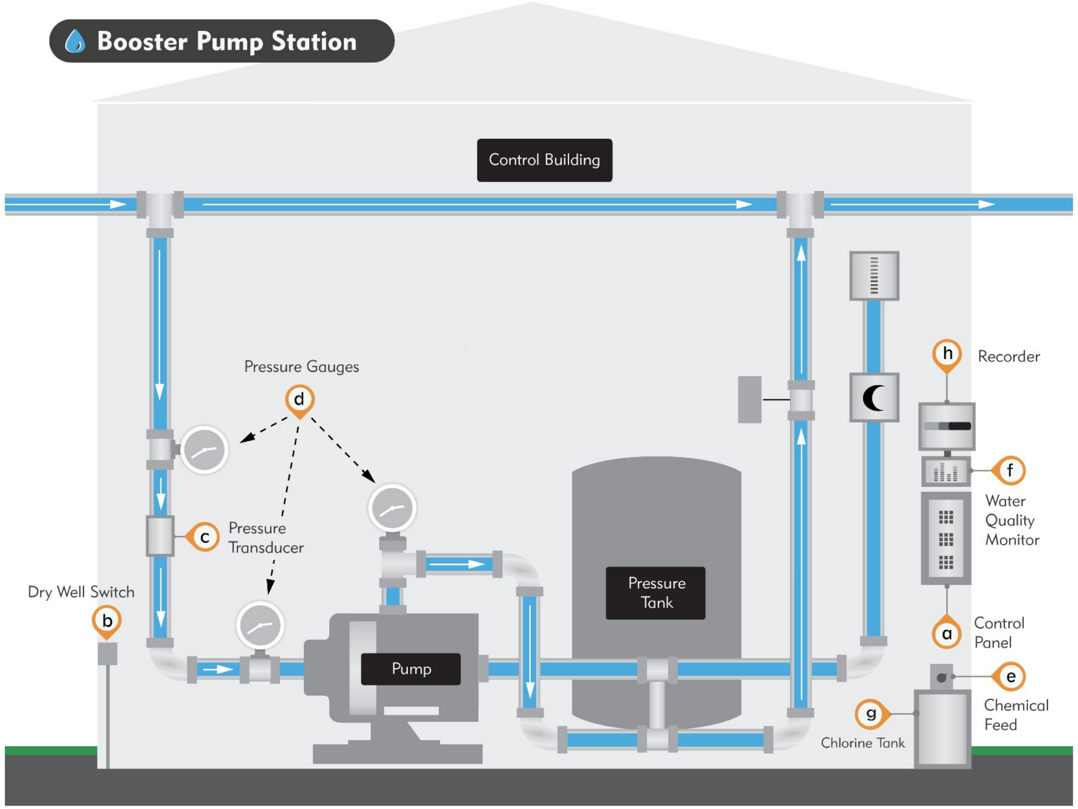
CIE Principles

Principle	Key Question
Consequence-Focused Design	How do I understand what critical functions my system must ensure and the undesired consequences it must prevent?
Engineered Controls	How do I implement controls to reduce avenues for attack or the damage which could result?
Secure Information Architecture	How do I prevent undesired manipulation of important data?
Design Simplification	How do I determine what features of my system are not absolutely necessary?
Layered Defenses	How do I create the best compilation of system defenses?
Active Defense	How do I proactively prepare to defend my system from any threat?
Interdependency Evaluation	How do I understand where my system can impact others or be impacted by others?
Digital Asset Awareness	How do I understand where digital assets are used, what functions they are capable of, and our assumptions about how they work?
Cyber-Secure Supply Chain Controls	How do I ensure my providers deliver the security we need?
Planned Resilience	How do I turn “what ifs” into “even ifs”?
Engineering Information Control	How do I manage knowledge about my system? How do I keep it out of the wrong hands?
Cybersecurity Culture	How do I ensure that everyone performs their role aligned with our security goals?

How does this work in practice?

Water Booster Pump Station

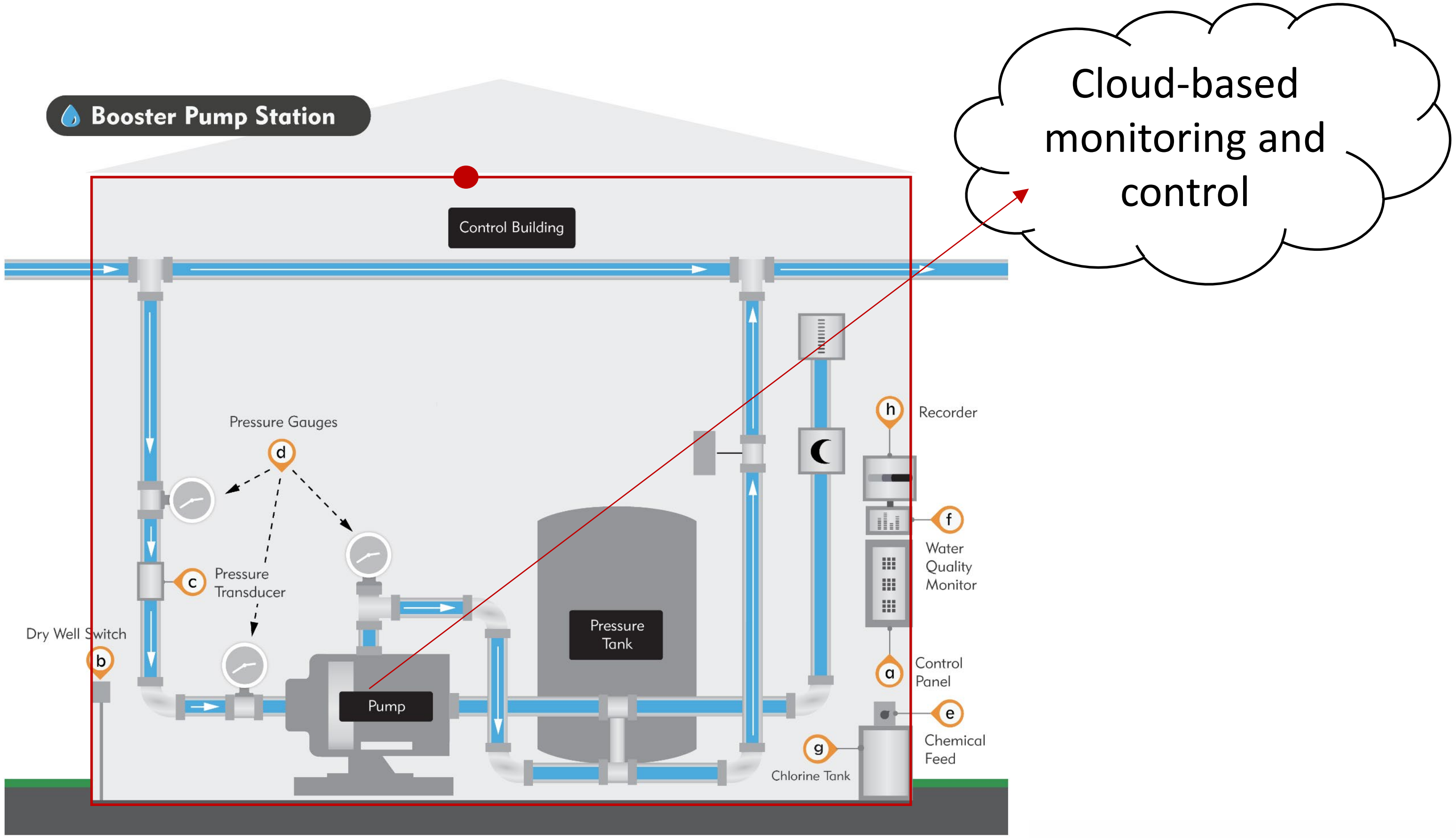
Water Booster Pump Station



Water Booster Pump Station Archives App4Water

https://www.app4water.com/product-category/applications/booster-pump-station/

Water Booster Pump Station



Cloud-based monitoring and control

Water Booster Pump Station Archives App4Water

https://www.app4water.com/product-category/applications/booster-pump-station/

Cyber Solution Review

- Control System Software has a qualifying secure development lifecycle.
  - Very mature demonstrated processes
  - Provided SBOM
  - Component infrastructure is up to date
  - Mature vulnerability release process – with regular patches
  - 24/7 Support availability

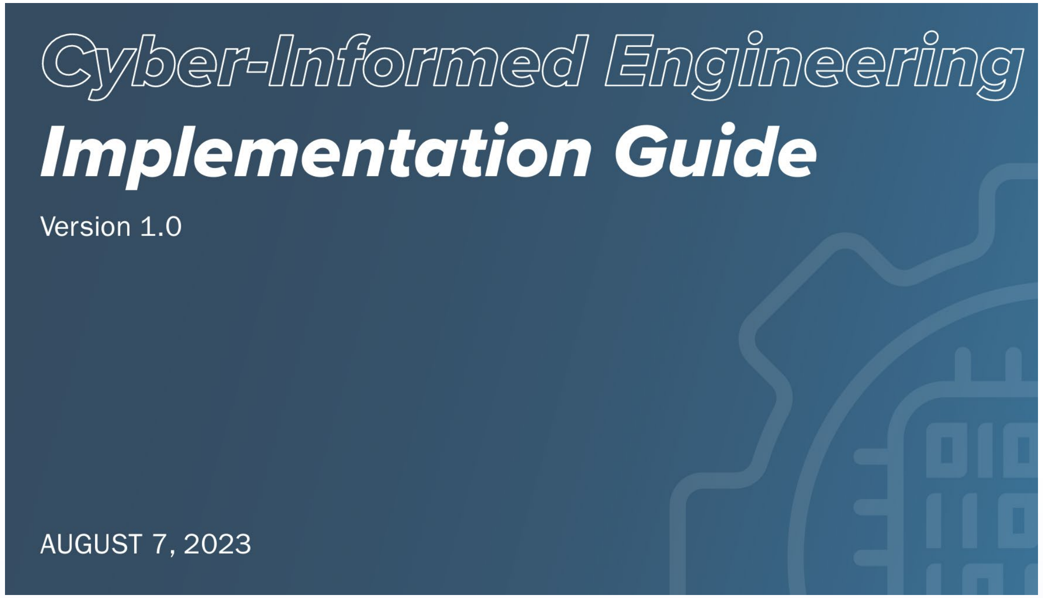
- Cloud provider is reputable and qualified
  - SOC Type 2 and FedRamp (if needed), great physical security
  - Very mature, experienced in hosting critical infrastructure services
  - Demonstrated response and restoration capabilities

IT Installation Review

- Network entry point has standard security package
- Monitoring and logging traffic on this interface according to standard practice
  - Logging interfaces with organizational logging system
- Traffic in and out is encrypted between the cloud provider and the site network boundary

Organizational Review Board Votes

- Finance / Accounting – ☑
- Information Technology – ☑
- Cybersecurity – ☑
- Engineering Operations – ? ➡



Cyber-Informed Engineering

Implementation Guide

Version 1.0

AUGUST 7, 2023

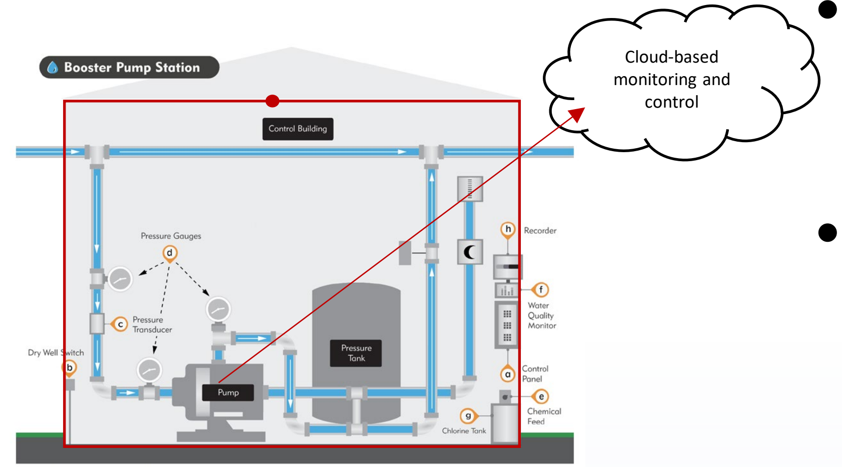
CIE Application for

Water Booster Pump Station

Consequence-Focused Design

KEY QUESTION

How do I understand what critical functions my system must ensure and the undesired consequences it must prevent?



Cloud-based monitoring and control

Water Booster Pump Station Archives App4Water

https://www.app4water.com/product-category/applications/booster-pump-station/

Assuming attacker defeats security controls:

- What is the worst that can happen?
- How would we respond?
- Would any of these issues be catastrophic?

Engineered Controls

KEY QUESTION

How do I implement controls to reduce avenues for attack or the damage which could result?

Attacker defeats security and turns pumps on / off quickly to damage equipment – 18-month outage, large repair / replacement project

- Ideal control:
  - Deterministic (governed by physics)
  - Not networked / digital
  - It is visible and can be seen in infrastructure
  - Complimentary with existing protections

What could we use?

Engineered Controls

KEY QUESTION

How do I implement controls to reduce avenues for attack or the damage which could result?

https://www.automationdirect.com/adc/shopping/catalog/relays_-z-_timers/timer_relays/trm-16-d-24ad#images-1

Attacker defeats security and turns pumps on / off quickly to damage equipment – 18-month outage, large repair / replacement project

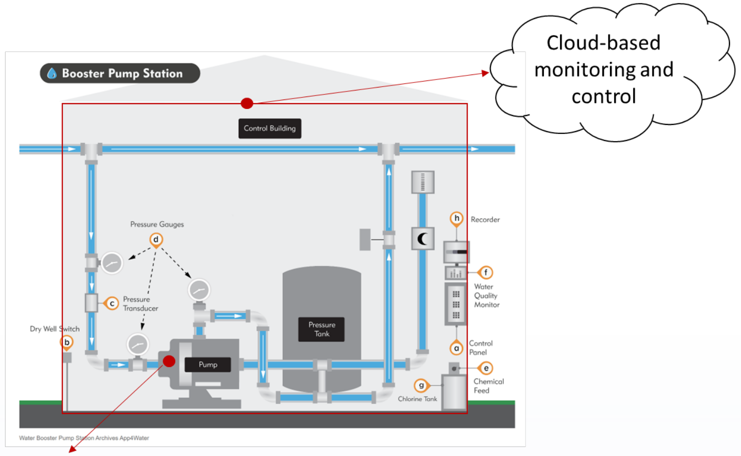
- Ideal control:
  - Deterministic (governed by physics)
  - Not networked / digital
  - It is visible and can be seen in infrastructure
  - Complimentary with existing protections

What could we use?

Secure Information Architecture

KEY QUESTION

How do I prevent undesired manipulation of important data?



Mechanical Time Delay Relay

https://www.app4water.com/product-category/applications/booster-pump-station/

What are the data elements in this system where manipulation could have the most impact?

- *IT says: Denial / Loss of View or Denial / Loss of Control*

Where could manipulation of data lead to Engineering or Operational Impacts?

- Loss of Protection
- Loss of Safety
- Loss of Productivity and Revenue
- Damage to Property

How should the potential for these specific operational impacts inform the cybersecurity strategy?

Cyber-Informed Engineering

Design Simplification

KEY QUESTION

How do I determine what features of my system are not absolutely necessary?

VFD-driven Pump

(1) https://www.automationdirect.com/adc/shopping/catalog/drives_-a-_soft_starters/ac_variable_frequency_drives_(vfd)/general_purpose_vfds/gs21-10p2#images-1

Where could we eliminate a system feature that would reduce potential for attack impacts? If we can't eliminate the features, how can we ensure they are not misused?

- When this pump station was built, the team considered a network-connected, Variable Frequency Drive-controlled pump.

Was there potentially a simpler design?

What are the feature trade-offs of the alternatives?

Design Simplification

KEY QUESTION

How do I determine what features of my system are not absolutely necessary?

VFD-driven Pump

Relay-driven Pump

(1) https://www.automationdirect.com/adc/shopping/catalog/drives_-a-_soft_starters/ac_variable_frequency_drives_(vfd)/general_purpose_vfds/gs21-10p2#images-1

(2) https://www.automationdirect.com/adc/shopping/catalog/relays_-z-_timers/electro-mechanical_relays/oa5611-52-24#images-1

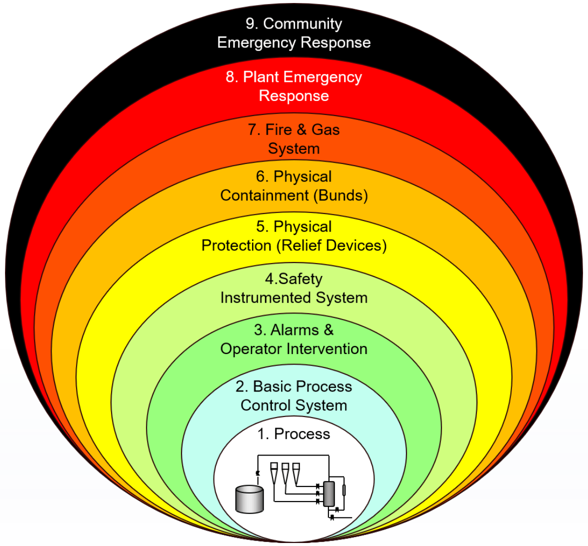
Where could we eliminate a system feature that would reduce potential for attack impacts? If we can't eliminate the features, how can we ensure they are not misused?

- When this pump station was built, the team considered a network-connected, Variable Frequency Drive-controlled pump.
- The team chose instead to have a relay control the pump.

Layered Defenses

KEY QUESTION

How do I create the best compilation of system defenses?


9. Community Emergency Response
8. Plant Emergency Response
7. Fire & Gas System
6. Physical Containment (Bunds)
5. Physical Protection (Relief Devices)
4.Safety Instrumented System
3. Alarms & Operator Intervention
2. Basic Process Control System
1. Process

https://www.thesafetymaster.com/risk-management/lopa-sil/

If we identify that an adversary turning on and off pumps leads to our worst engineering consequences -

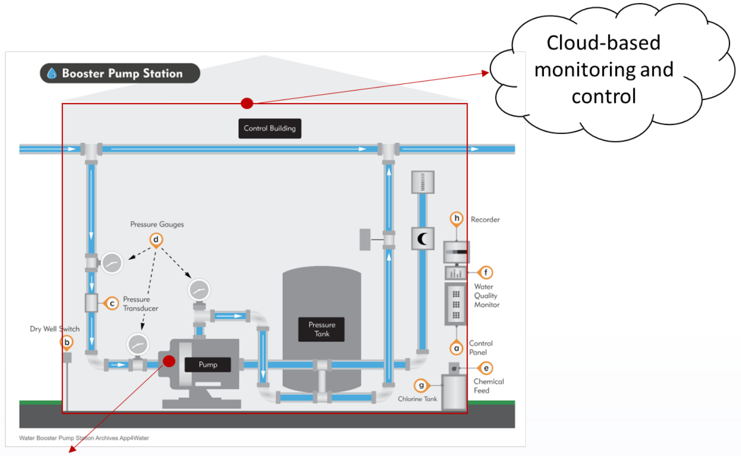
- How can cybersecurity prioritize the defenses from our side and from the vendors to detect or prevent that from happening?
- How many layers of protection can we assemble?
- How can we inform cybersecurity requirements?

Cyber-Informed Engineering

Active Defense

KEY QUESTION

How do I proactively prepare to defend my system from any threat?



Cloud-based monitoring and control

Water Booster Pump Station Archives App4Water

Mechanical Time Delay Relay

If we identify that an adversary turning on and off pumps leads to our worst engineering consequences -

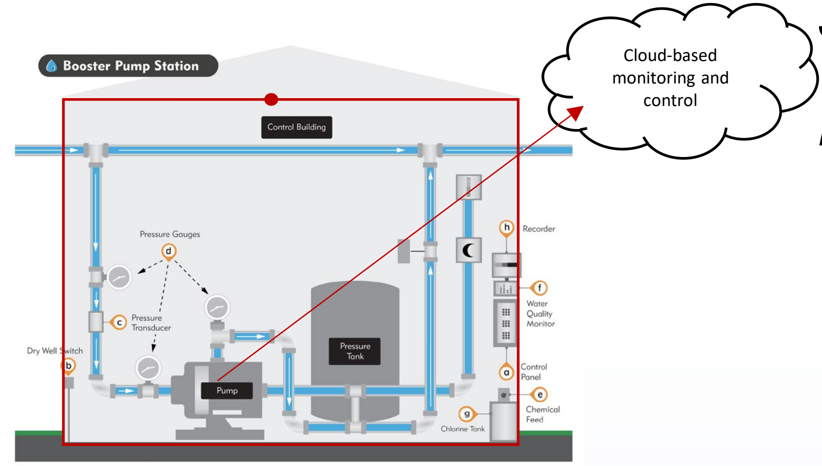
- How would we defend against that action?
- What do we expect of our vendor? Do we need additional contracts?
- How will engineering and cyber work together during the defense?
- Have we documented and practiced our defense?

https://www.thesafetymaster.com/risk-management/lopa-sil/

Interdependency Evaluation

KEY QUESTION

How do I understand where my system can impact others or be impacted by others?



Cloud-based monitoring and control

Water Booster Pump Station Archives App4Water

https://www.app4water.com/product-category/applications/booster-pump-station/

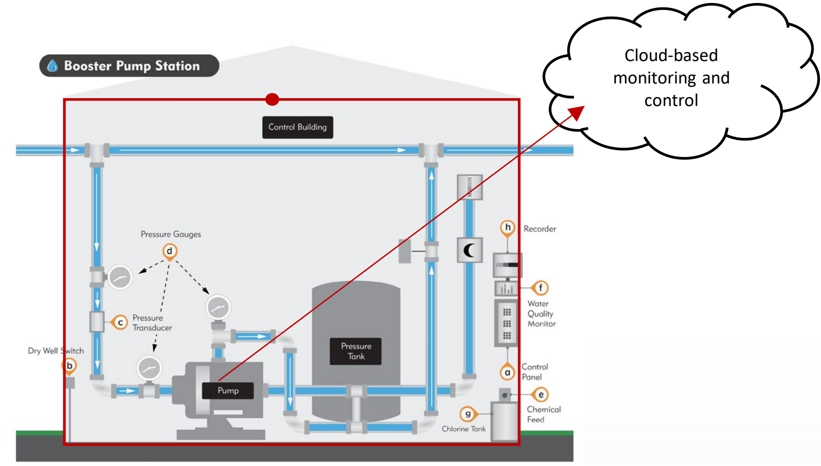
We have added a new interdependency – the cloud service and software. Beyond specific cyber attack, how might instability in this service affect our operations?

- What happens if the service goes down?

Digital Asset Awareness

KEY QUESTION

How do I understand where digital assets are used, what functions they are capable of, and our assumptions about how they work?



Water Booster Pump Station Archives App4Water

https://www.app4water.com/product-category/applications/booster-pump-station/

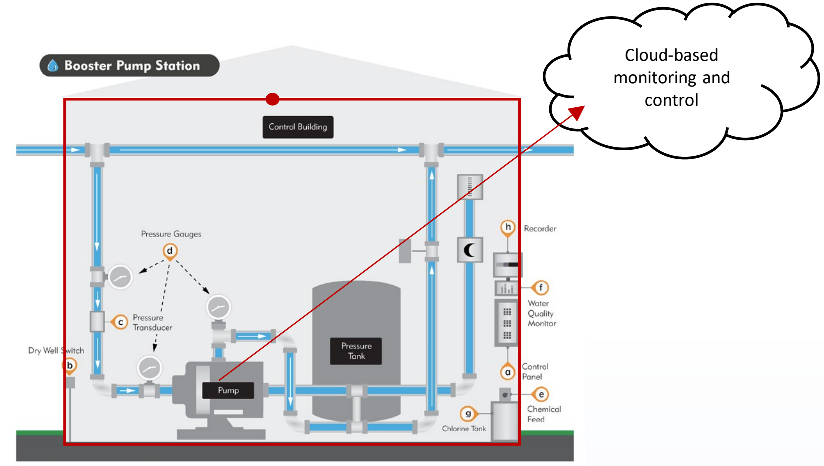
We have talked to the vendor about extending the product to allow remote control of the chlorinator. We are used to operating it manually. How will the use of digital technology change engineering risk?

- Is the dispensed amount hardwired or adjustable?
- How do we know that the product was actually dispensed?

Cyber-Secure Supply Chain Controls

KEY QUESTION

How do I ensure my providers deliver the security we need?



Cloud-based monitoring and control

Water Booster Pump Station Archives App4Water

https://www.app4water.com/product-category/applications/booster-pump-station/

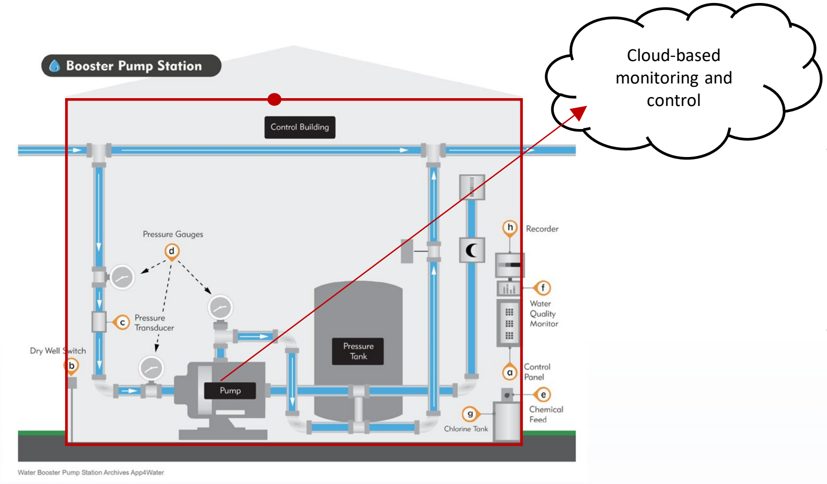
We examined the components used by the vendor and the security culture of the cloud company and both were very mature. However, there are still some questions we need to ask.

- How is the system patched? How are patches delivered? Can the asset owner accept or reject a patch?
- Does the software vendor or cloud provider ever allow access to our system to their vendors or maintainers?
- How are 3rd-party support providers, including the call-in support qualified and vetted?
- What else?

Planned Resilience

KEY QUESTION

How do I turn "what ifs" into "even ifs"?



Cloud-based monitoring and control

Water Booster Pump Station Archives App4Water

https://www.app4water.com/product-category/applications/booster-pump-station/

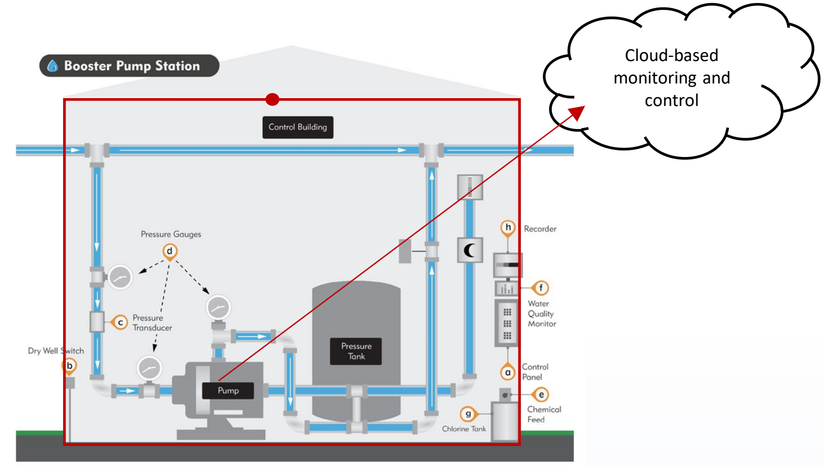
- *What if an attacker turned all of the pumps on or off?*
  - ??
- *What if the application vendor reported an adversary attack?*
  - ??
- *What if the application stopped working?*
  - ??
- *What if the cloud vendor had ransomware?*
  - ??

Planned Resilience

KEY QUESTION

How do I turn “what ifs” into “even ifs”?

- *What if an attacker turned all of the pumps on or off?*
  - We use manual operations and contact the vendor. We predict very little loss from this scenario.
- *What if the application vendor reported an adversary attack?*
  - We return to manual operations and have a contract vehicle to ensure we can staff that for up to 2 weeks.
- *What if the application stopped working?*
  - See above. After two weeks, we would need to arrange for emergency staffing.
- *What if the cloud vendor had ransomware?*
  - See above.



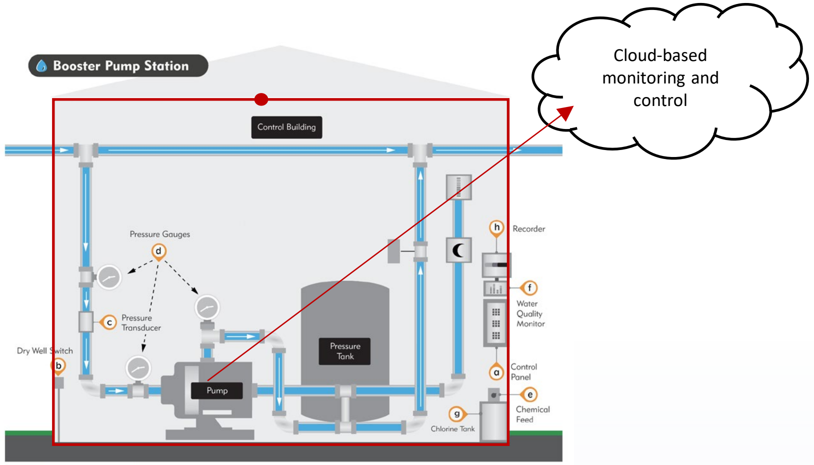
Water Booster Pump Station Archives App4Water

https://www.app4water.com/product-category/applications/booster-pump-station/

Engineering Information Control

KEY QUESTION

How do I manage knowledge about my system? How do I keep it out of the wrong hands?



Water Booster Pump Station Archives App4Water

https://www.app4water.com/product-category/applications/booster-pump-station/

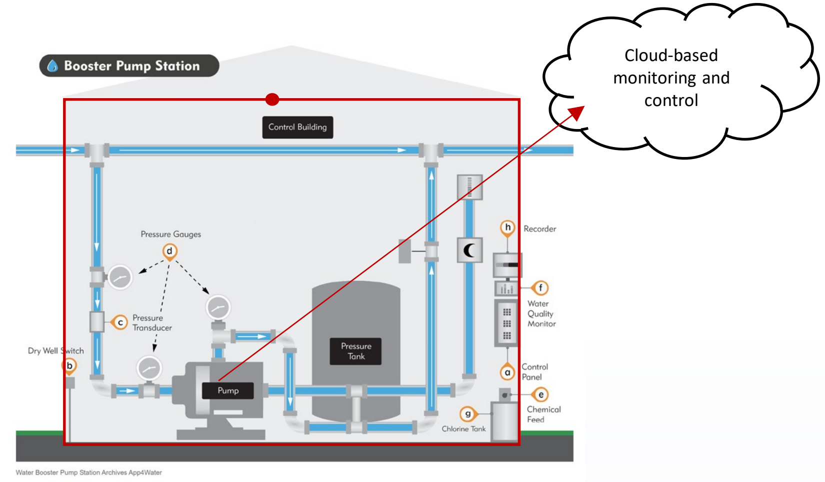
- *How much information about this upgrade must be shared*?
  - Municipal water activities are public record.
  - High level information about this upgrade must be shared.
  - What should we share and what should we withhold?

Cyber-Informed Engineering

Engineering Information Control

KEY QUESTION

How do I manage knowledge about my system? How do I keep it out of the wrong hands?



Water Booster Pump Station Archives App4Water

https://www.app4water.com/product-category/applications/booster-pump-station/

- *How much information about this upgrade must be shared*?
  - Municipal water activities are public record.
  - High level information about this upgrade must be shared.
  - Engineering team recommends to leadership that the specific vendor, product name, and cloud vendor name be kept out of the record.

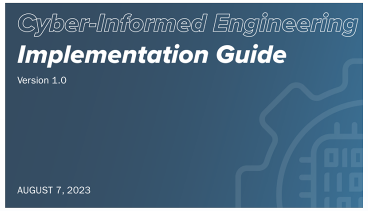
Cybersecurity Culture

KEY QUESTION

How do I ensure that everyone performs their role aligned with our security goals?

Organizational Review Board Votes

- Finance / Accounting – ☑
- Information Technology – ☑
- Cybersecurity – ☑
- Engineering Operations – ? ➡



Cyber-Informed Engineering

Implementation Guide

Version 1.0

AUGUST 7, 2023

- *How do we build an inclusive cybersecurity culture?*
  - The fact that engineering could drive the implementation based on potential impacts of a cyber attack was a major change.
  - What functions within our organization are critical to our security? What do we need them to know / do?

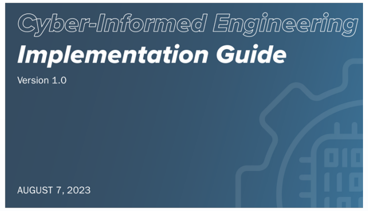
Cybersecurity Culture

KEY QUESTION

How do I ensure that everyone performs their role aligned with our security goals?

Organizational Review Board Votes

- Finance / Accounting – ☑
- Information Technology – ☑
- Cybersecurity – ☑
- Engineering Operations – ? ➡



Cyber-Informed Engineering

Implementation Guide

Version 1.0

AUGUST 7, 2023

- *How do we build an inclusive cybersecurity culture?*
  - The fact that engineering could drive the implementation based on potential impacts of a cyber attack was a major change.
  - Engineering will need to talk to procurement to ensure resiliency resources are obtained.

So Where from here with CIE?

CIE Implementation Guide

https://www.osti.gov/servlets/purl/1995796

U.S. DEPARTMENT OF ENERGY | Offi Cy an

Cyber-I

Implem

Version 1.0

DRAFT

AUGUST 7, 2023

PRINCIPLE 1
Consequen

KEY QUESTION
How do I understand
ensure and the unde

Principle Description

Apply CIE strategies first and foremost to the m system performs. Typically these are functions subverted, could result in unacceptable or cata the organization, including undesired impacts t environment, availability or effectiveness of pro integrity, and public image. Use a structured ar areas where digital technology is used within th

Consider where an unprotected action or failure digital technology might lead to a high-consequ include unauthorized system actions, invalid da automated action, or interdiction of a digitally g controls that exist to minimize impacts of misu controls are implemented via digital technology combination of both.

This list of high-impact consequences underpin perform throughout the system design lifecycle and their priority within each CIE principle. For the work above, engineers will consider engine 2: Engineered Controls), that could either remo unprotected action or mitigate its consequence

[4] This idea aligns with ISA/IEC 62443 "Assess, Design While the system may not have changed, the patches unconsidered consequences. The reassessment shou

Cyber-Informed Engineering Implementation Guide | Version

PRINCIPLE 1
PHASE A

PRINCIPLE 1: CONSEQUENCE
CONCEPT PHASE (continued)

5 **What business**
a Which part consequen
b Which resu "acceptabl risk manag
c Which cons "unaccepta distinct cor

6 **What regional system failure**
a What entiti infrastructu
b What chan from regior

7 **What crucial as**
a What violat

8 **Where might ro**
a At each ins

9 **Are there adver**
a What circu
b In adverse consequen

10 **What staffing r What training c**
a Where mig support or
b What are t

Cyber-Informed Engineering Imp

First point in the Engineering Lifecycle that the example is considered ■

Continuation of the example through the Engineering Lifecycle ▨

		CIE Engineering Lifecycle					
		Concept	Requirements	Design	Development	Testing, Verification, Validation, and Deployment	Operations and Maintenance
		Water Sector Engineering Lifecycle					
PRINCIPLE	**CIE CONTROL/MITIGATION EXAMPLE**	Planning Concept	Preliminary Design Report	Detailed Design	Construction and Commissioning		Operations and Maintenance
Principle 6: Active Defense	**6-1** Implement an OT network monitoring solution. Design network to support data collection by sensors. Employ Zero Trust Architecture where possible.					■	▨
	6-2 Generate documentation on how to detect early warning signs and how to block, disconnect, and isolate network connection/device(s).					■	▨
Principle 7: Interdependency Evaluation	**7-1** Implement continuous inter-departmental training to build relationships between different disciplines which will facilitate communication during emergency situations.					■	▨
	7-2 Ensure multiple sources are available for any dependency on outside inputs.		■	▨	▨	▨	▨
Principle 8: Digital Asset Awareness	**8-1** Adopt a commercial off the shelf OT network monitoring solution that uses passive data collection to build an asset inventory.					■	▨
	8-2 Regularly update the software and firmware on all devices found in the inventory					■	▨
Principle 9: Cyber-Secure Supply Chain Controls	**9-1** Include security requirements in RFPs and contracts, develop a Secure Software Lifecycle Development program and implement tight vendor controls.				■	▨	▨
Principle 10: Planned Resilience	**10-1** Install hardwired controls for all critical systems.			■	▨	▨	▨
	10-2 Generate documentation and train staff to expect that any digital component can become compromised and lose functionality and know how to operate in manual.					■	▨

Cyber-Informed Engineering Implementation Guide | Version 1.0 - DRAFT 166