ENERGY NORTHWEST

Cyber Security Device Lifecycle Management

Presenter: Jason Davis and Kevin Sykes

July 29, 2019

Notice: This document may contain Confidential/Proprietary/Trade Secret Information ("Confidential Information") of the Institute of Nuclear Power Operations, the Utilities Service Alliance, Inc. or the World Association of Nuclear Operations. Confidential Information shall not be disclosed outside of Energy Northwest by any employee, contractor or employee of a contractor except as expressly provided in SWP-REC-03.

Regulatory Basis

Regulation: 10CFR 73.54

Industry Guidance (NRC endorsed): NEI 08-09 Rev. 6 & Addendums 1-4

Station's License Basis Document

Defense-In-Depth Requirement

Defense-in-depth protective strategies have been implemented, documented, and are maintained to ensure the capability to detect, delay, respond to, and recover from cyber attacks on CDAs.

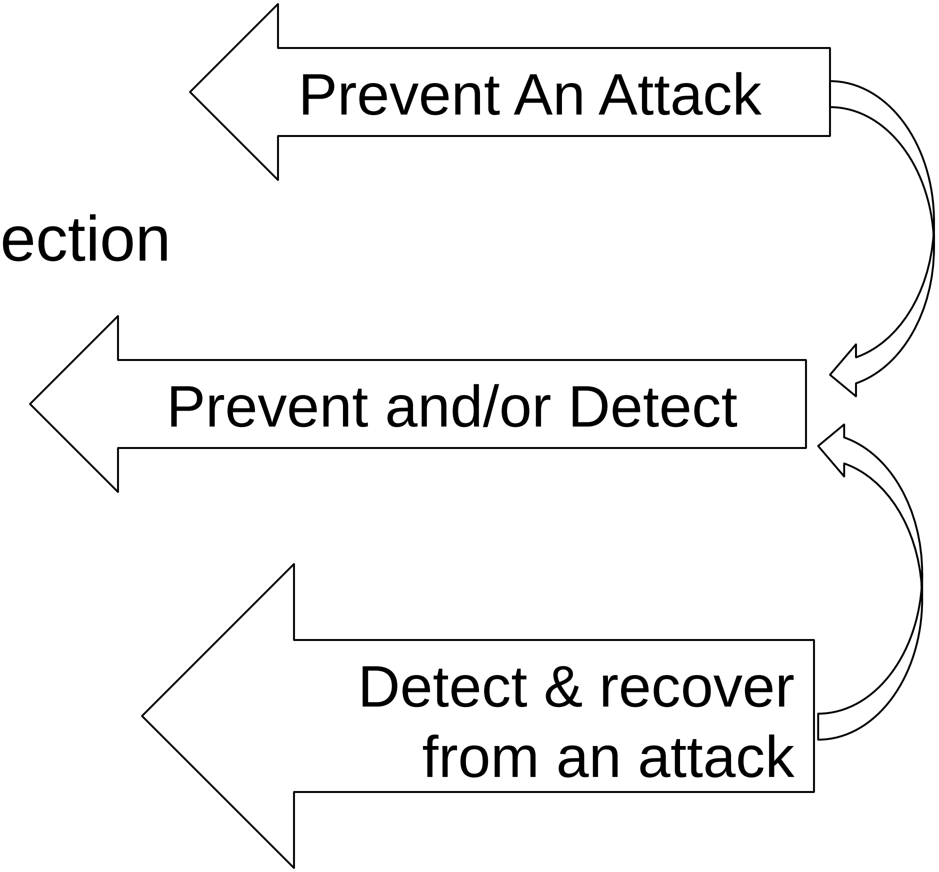
-NEI 08-09 Revision 6, Appendix A, Section 4.3

Defense-In-Depth Strategy

1. Physical Protection
2. Network Protection
3. Portable Media / Device Protection
4. Individual CDA Protections
5. Monitoring and Detection
6. Incident Response

Defense-In-Depth Strategy

1. Physical Protection
2. Network Protection
3. Portable Media / Device Protection
4. Individual CDA Protections
5. Monitoring and Detection
6. Incident Response



Prevent An Attack

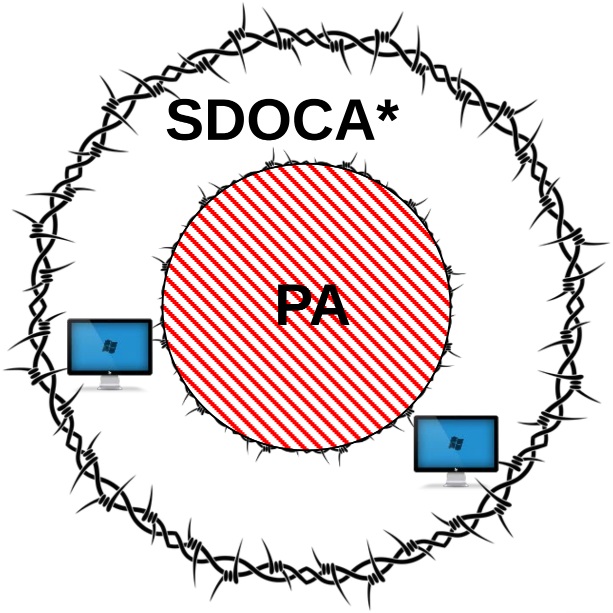
Prevent and/or Detect

Detect & recover from an attack

Physical Protection

The 1st layer of protection for Critical Digital Assets (CDAs) is to provide physical protection.

Only addressed for CDAs outside the PA.

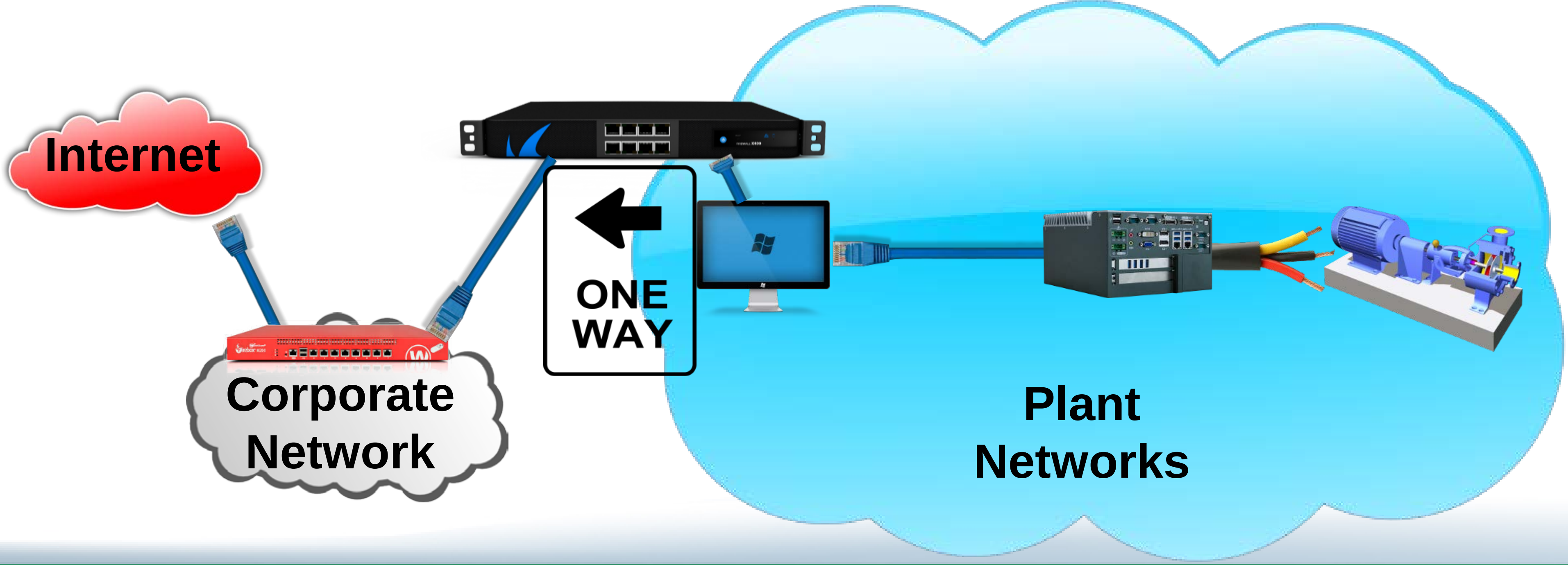


*Site defined owner controlled area

Network Protection

The 2nd layer of protection for Critical Digital Assets (CDAs) is to isolate/segment network access.

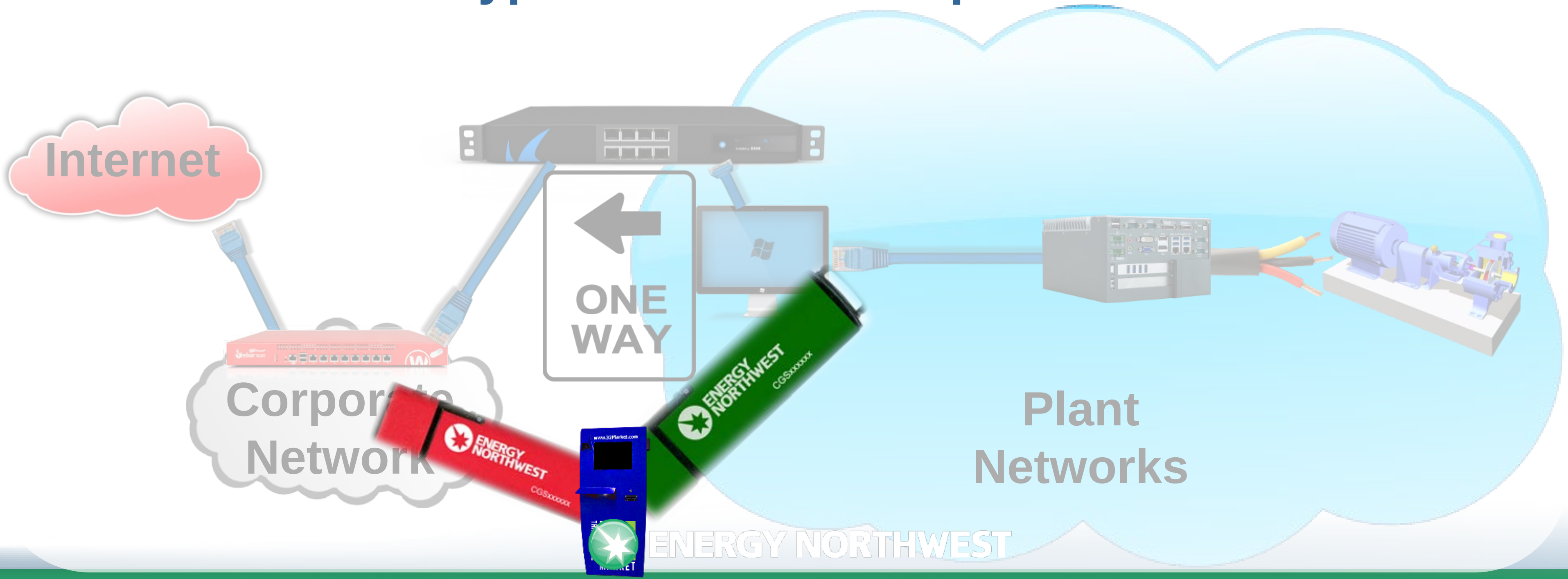
This eliminates the easiest path to attack CDAs – remote attacks that bypass physical security protections



Portable Media / Device Protection

The 3rd layer of protection is to control portable media and devices.

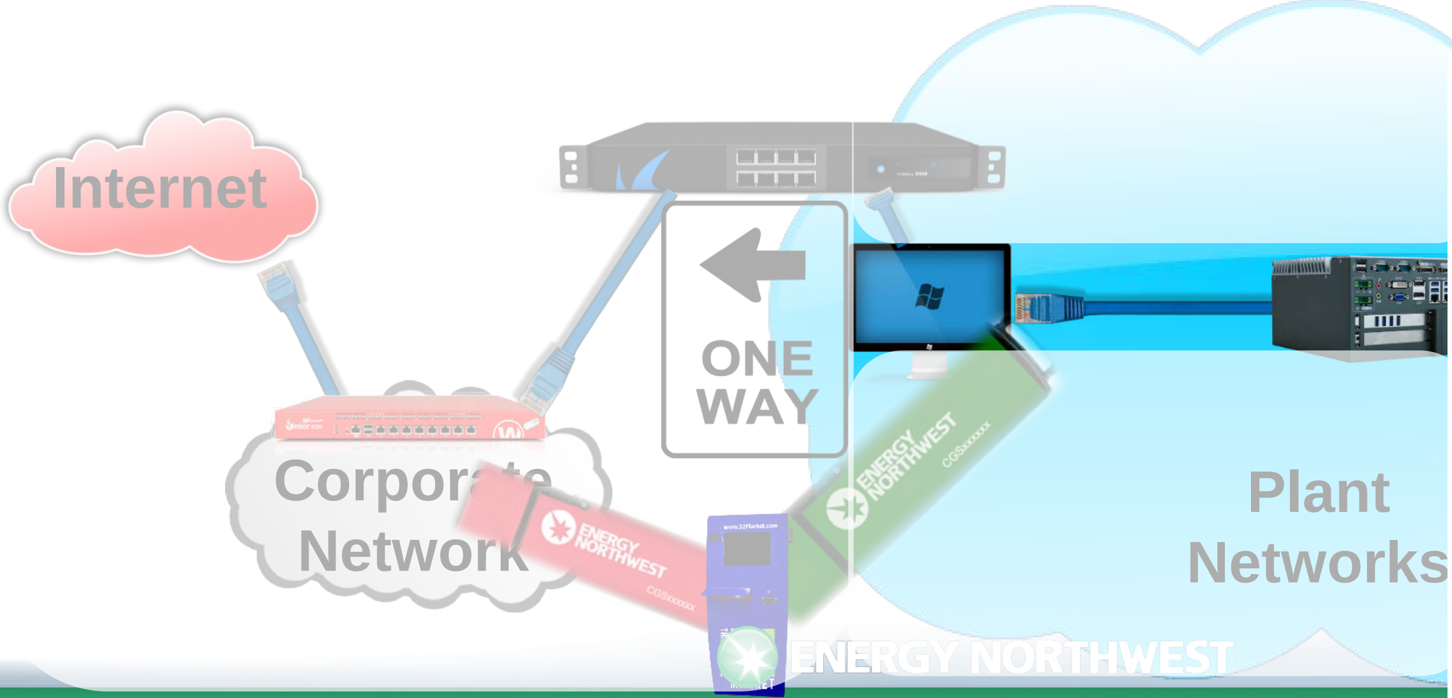
This controls the "approved" way for authorized personnel to bypass the network protections



Individual CDA Protection

The 4th layer of protection is to apply security controls directly to each CDA.

This provides a high degree of protection but presents a significant operational challenge on legacy systems.



Examples

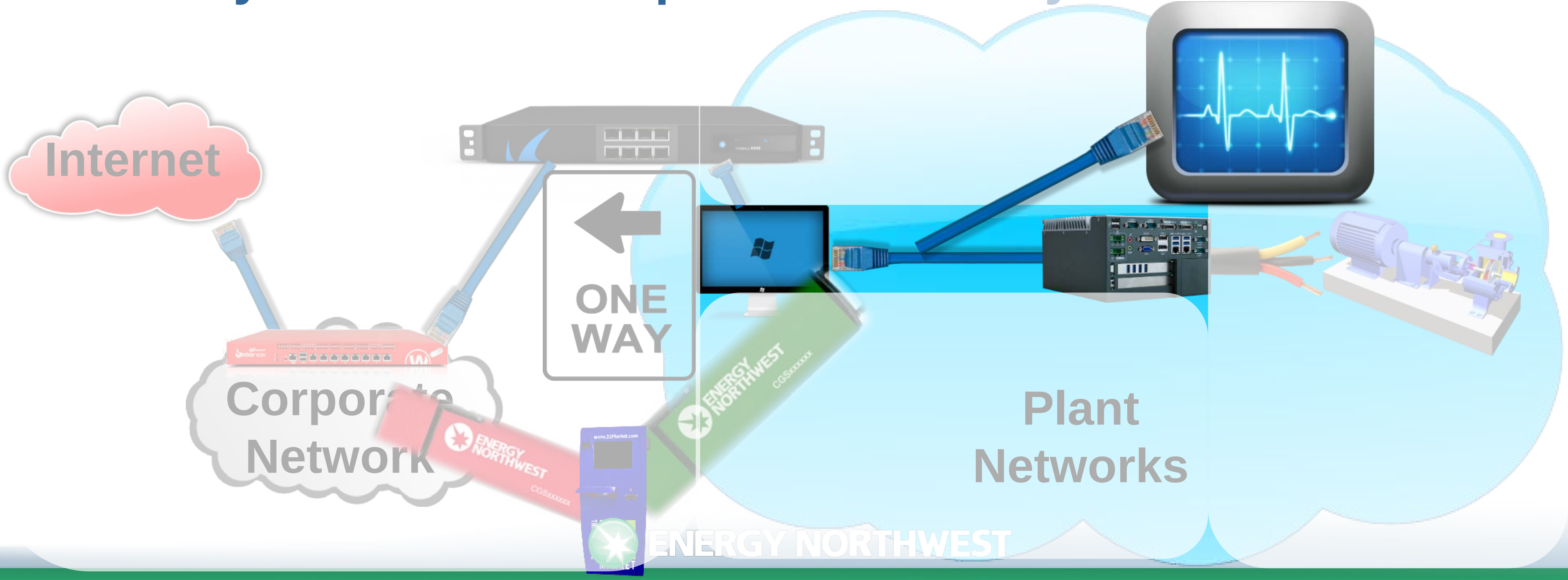
- Passwords
- Antivirus
- Individual Accounts
- Logging & Auditing
- Whitelisting

Notice: This document may contain Confidential/Proprietary/Trade Secret Information ("Confidential Information") of the Institute of Nuclear Power Operations, the Utilities Service Alliance, Inc. or the World Association of Nuclear Operations. Confidential Information shall not be disclosed outside of Energy Northwest by any employee, contractor or employee of a contractor except as expressly provided in SWP-REC-03.

Monitoring & Detection

The 5th layer of protection is to add centralized network monitoring to identify cyber events across multiple CDAs.

This is a reactive control that minimizes impact by enabling timely detection & response when a cyber event occurs

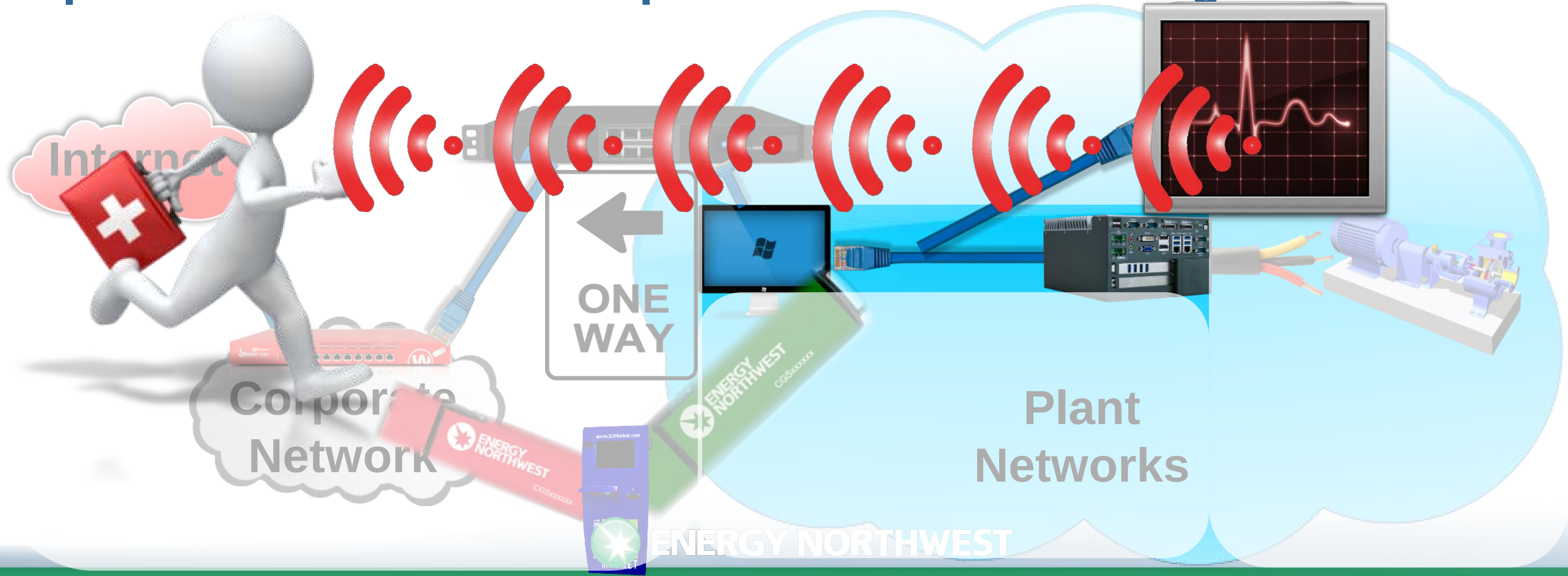


Notice: This document may contain Confidential/Proprietary/Trade Secret Information ("Confidential Information") of the Institute of Nuclear Power Operations, the Utilities Service Alliance, Inc. or the World Association of Nuclear Operations. Confidential Information shall not be disclosed outside of Energy Northwest by any employee, contractor or employee of a contractor except as expressly provided in SWP-REC-03.

Incident Response

The 6th layer of protection is ensure trained personnel are available to respond when a cyber event is detected

This is a reactive control that minimizes impact by ensuring qualified individuals respond to contain & mitigate an event.



Cyber Security Modifications

Stations performed numerous cyber security modifications to implement the requirements of 10 CFR 73.54.

Cyber Security Modifications

These modifications primarily addressed:

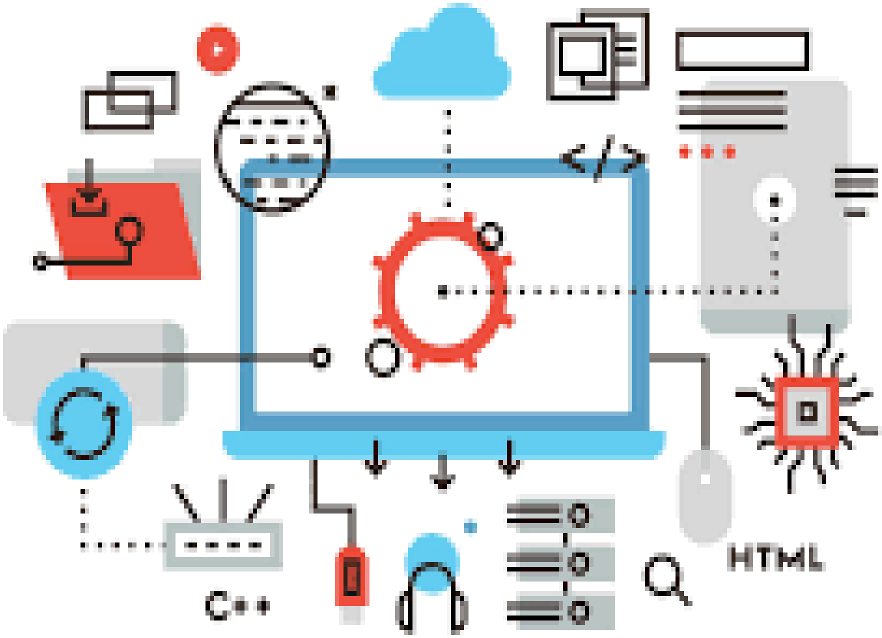
1. Physical Protection
2. Network Protection
3. Portable Media / Device Protection
4. Individual CDA Protections
5. Monitoring and Detection
6. Incident Response

Future Cyber Security Modifications

Two issues will drive future Cyber Security modifications

1. Vulnerability Monitoring

2. Cyber Security Device Obsolescence



Notice: This document may contain Confidential/Proprietary/Trade Secret Information ("Confidential Information") of the Institute of Nuclear Power Operations, the Utilities Service Alliance, Inc. or the World Association of Nuclear Operations. Confidential Information shall not be disclosed outside of Energy Northwest by any employee, contractor or employee of a contractor except as expressly provided in SWP-REC-03.

Vulnerability Monitoring

Hardware and software vulnerabilities are reported to the federal government and published every day.

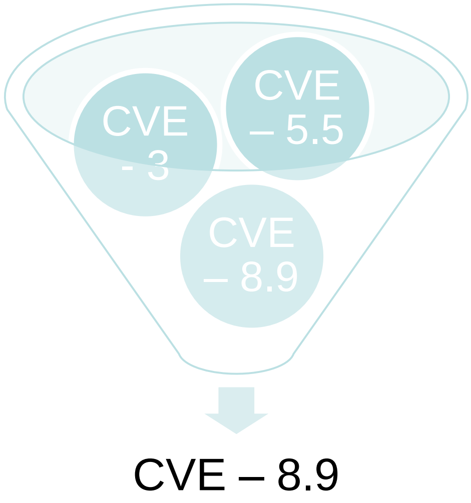
We are obligated to screen all of these vulnerabilities to determine what vulnerabilities exist on hardware/software in use at Columbia.

Industry had developed a database that could be used by every utility to simplify this process, but this has been deemed unreliable during the inspection process.

Vulnerability Monitoring Process

1. **Obtain the list of weekly vulnerabilities (> 100/week)**

2. **Screen out any with a severity score of less than 7 for most CDAs**



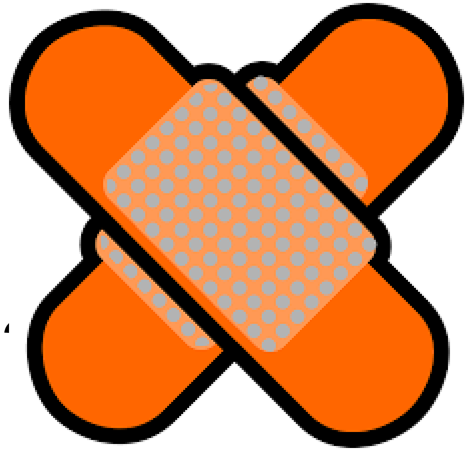
3. **Determine which vulnerabilities apply to site (hardware or software)**

4. **Review the applicable vulnerabilities and document an assessment of whether that vulnerability is adequately addressed by the current security controls**

Vulnerability Remediation

Vulnerabilities that are not adequately addressed by our current security controls, require a change to address the vulnerability.

Typically, this will require a software patch.



What method is used to implement the patch?

- Complete Engineering Change
- Create a Procedure that can be used

If a cyber event occurs due to an unpatched vulnerability it can escalate the color severity of the finding.

Cyber Security Device Obsolescence

For cyber security, some devices need to be replaced within a normal IT lifecycle. This includes:

1. Boundary device (diode, firewall, or network tap)
2. Provides central monitoring function that requires vendor support/updates to be current with evolving threats (e.g., SIEM, anti-virus, network switches with intrusion detection, etc.)

Cyber Security Device Obsolescence

Equipment inventory

1. **Boundary devices:**
2. **Central monitoring functions:**

Typical replacement lifecycle is 6-8 years.

Equipment should qualify as like-for-like replacement

QUESTIONS

Notice: This document may contain Confidential/Proprietary/Trade Secret Information ("Confidential Information") of the Institute of Nuclear Power Operations, the Utilities Service Alliance, Inc. or the World Association of Nuclear Operations. Confidential Information shall not be disclosed outside of Energy Northwest by any employee, contractor or employee of a contractor except as expressly provided in SWP-REC-03.

ENERGY NORTHWEST