SECURITY PROGRAM ASSESSMENT REPORT

Aspen Creek Power and Water

Mitchell Dees
High Plains Security Consulting

Current Environment Overview

Core Organization Operations

- Power Distribution
- Water Treatment
- Water Distribution
- Utilities Usage Monitoring
- Customer Billing
- Network Monitoring and Maintenance
- General IT Service
- Administrative Service

Core Organization Assets

- **Aspen Creek Power and Water Headquarters**
    - Headquarter Employees
    - Headquarter Employee Badges
    - Headquarters CCTV
    - Organization Servers
    - Headquarters LAN
    - Network Operations Center Systems
    - Network Operations Center Employees
    - Administrative Information Systems
    - Employee Laptops
    - Employee Data
    - Customer Data
    - Sensitive Organization Data
    - HR Cloud System
    - Billing Cloud System

- **Electric Substation**
    - Electric Substation Employees
    - Electric Substation Employee Badges
    - Electric Substation CCTV
    - Electric Substation SCADA/OT Network
    - Electric Substation Information Systems
    - Electric Substation Mechanical Systems
    - Electric Substation Sensitive Data

- **Water Treatment Plant 1 & 2**
    - Water Treatment Employees
    - Water Treatment Plant 1 Keypad Code
    - Water Treatment Plant 2 Employee Badges
    - Water Treatment Plant CCTV
    - Water Treatment Plant SCADA/OT Network
    - Water Treatment Information Systems
    - Water Treatment Mechanical Systems
    - Water Treatment Plant Sensitive Data

Current Security Measures in Place

Physical

- Badge exterior door access system
- Keypad exterior door access system
- Locked exterior doors for remote sites
- Locked doors for headquarters outside of normal business hours
- CCTV systems for all four organization sites

Technical

- Firewall
- Access Control Software

Administrative

- None reported in the environment overview

NIST 800-53 Gap Analysis

AC-17(2) Protection of Confidentiality and Integrity Using Encryption

According to the current environment overview, about a third of Aspen Creek Power and Water‘s employees engage in remote work practices at least two days a week. Aspen Creek Power and Water’s current security program includes no mention of any security controls protecting remote access to organization assets. The absence of security controls indicates that the organization security program does not align with AC-17(2): Protection of Confidentiality and Integrity Using Encryption, which states that organizations should “implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions” (CSF Tools, 2024).

Recommended Action

The main recommendation for compliance with NIST 800-53 AC-17(2) is to set up an organization VPN with a VPN service provider for encrypted and secure connections to internal organization networks, systems, and data. All workstations, laptops, and other systems used by Aspen Creek Power and Water employees engaging in remote work should connect to internal organization assets and cloud resources through the organization VPN.

Implementation Plan

Immediate:	Ensure remote access for work is done on private networks using secure protocols such as ssh
Short Term:	Find a suitable VPN vendor and engage in contract negotiations
Long Term:	Implement an organization VPN and force usage for remote work

MA-6(1) Preventative Maintenance

In the recent incidents section of the current environment overview, a scheduled preventative maintenance check on a firewall was not performed due to a perceived lack of time by IT personnel. This behavior is not compliant with MA-6(1), as it requires organizations to "Perform preventive maintenance on [Assignment: *organization-defined system components*] at [Assignment: *organization-defined time intervals*]" (CSF Tools, 2024). Additionally, the current organizational environment does not include a policy and procedures document that defines the frequency at which preventative maintenance must occur.

Recommended Action

The main recommendation for compliance with NIST 800-53 MA-6(1) is to establish policies and procedures in Aspen Creek Power and Water's security program to ensure that the regular maintenance and inspection of organizational systems, technical security controls, and networks are secure and functional.

Implementation Plan

Immediate:	Perform the missed preventative maintenance check
Short Term:	Develop and document proactive preventative maintenance policies and procedures
Long Term:	Monitor IT personnel adherence to new preventative maintenance policies and procedures through documentation of when preventative maintenance occurs and by whom

PE-6(3) Video Surveillance

According to a review of the current organization security environment, video surveillance is still operational at Aspen Creek Power and Water headquarters, but some cameras at the remote electric substation and water treatment plants are inoperable. Currently, the organization is not compliant with NIST 800-53 PE-6(3), as it requires the organization to "Employ video surveillance of [Assignment: *organization-defined operational areas*]" (CSF Tools, 2024). The control also contains requirements for reviewing and retaining video surveillance footage, but the main gap is the inoperable cameras not performing any actual surveillance.

Recommended Action

Aspen Creek Power and Water should look to overhaul their current camera system to stay compliant with NIST 800-53 PE-6(3). If a significant portion of security cameras are broken beyond repair due to age, environment, or camera quality, then the organization should simply acquire and install a new camera system. In the meantime, the organization should attempt to fix as many cameras as they can and find temporary replacements for those that are too broken to be fixed.

Implementation Plan

Immediate: Have IT or maintenance attempt to fix the current inoperable cameras

Short Term: Purchase temporary cameras to replace the current cameras that cannot be fixed

Long Term: Replace organization security cameras with newer, more resilient models

AC-2(9) Restrictions on Use of Shared / Group Accounts

Contractors working with Aspen Creek Power and Water collectively use a single login credential while accessing the SCADA network at the electric substation facility. The control AC-2(9) requires that organizations must “only permit the use of shared and group accounts that meet [Assignment: *organization-defined conditions*]” (CSF Tools, 2024) and recommends that “organizations consider the increased risk due to the lack of accountability with such accounts” (CSF Tools, 2024). Contractors, or malicious actors that obtain the login credential, may be able to lie about committing unlawful or negligent actions, resulting in a compromise of business operations and sensitive data traveling across the SCADA network.

Recommended Action

Aspen Creek Power and Water should deprovision the collective electric substation contractor SCADA network login credentials and provision every contractor with individual login credentials to enforce non-repudiation and remain compliant with NIST 800-53 AC-2(9). Additionally, the organization must implement monitoring systems and require periodic password changes to ensure that contractors are not sharing login credentials.

Implementation Plan

Immediate: Deprovision the collective electric substation contractor SCADA network log in credential

Short Term: Provision every electric substation contractor with new individual log in credentials

Long Term: Monitor electric substation SCADA network contractor log in credential usage along with requiring periodic password changes

PE-3(1) System Access

Inside the current environment of Aspen Creek Power and Water headquarters, interior office doors remain unlocked during regular business hours. A malicious actor with enough confidence and cunning could walk into areas of the office with information systems, servers, or other important assets unhindered. This is not compliant with the NIST 800-53 control PE-3(1), which requires the organization to "Enforce physical access authorizations to the system in addition to the physical access controls for the facility at [Assignment: *organization-defined physical spaces*]" (CSF Tools, 2024).

Recommended Action

To ensure compliance with PE-3(1), Aspen Creek Power and Water should ensure that all office doors with access to information systems are locked to those outside the organization and that only valid organization credentials open the doors. Additionally, the organization must determine which areas of the office do not have information systems and require public access like the lobby and bathrooms.

Implementation Plan

Immediate:	Require interior office doors to remain locked and secure even during business hours
Short Term:	Develop and document physical office security policies and procedures regarding system access
Long Term:	Monitor adherence to documented policies and procedures along with implementing badge-based door access controls if needed

Threat Risk Analysis

Threat	Impact	Likelihood	Risk Score	Risk Level
Lost Organization Laptop	4	2	8	Medium
Phishing Emails	4	5	20	High
Remote Facility Break-in	4	3	12	Medium

Threat 1: Lost Organization Laptop

The threat of a lost organization laptop is a medium-level risk to the Aspen Creek Power and Water organization. While the potential impact of a lost laptop is very high if a malicious actor obtains it, the likelihood of an employee losing their organization laptop remains relatively low. A malicious actor could exploit several vulnerabilities, such as a weak password or unencrypted hard drive, to gain access to other organization assets, data, and networks, which could compromise business operations. The likelihood score for the laptop would have been the lowest score, one, but due to the recent incident of the plant supervisor losing their organization laptop, the likelihood score was increased to two.

Recommended Action

The main action recommended for the loss of an organization laptop is to implement encryption of the laptop's hard drive or solid-state drive along with its memory. Implementing strong encryption of the laptop's data assets adheres to the NIST 800-53 control SC-13, which requires determining cryptographic uses and types for each use (CSF Tools, 2024). Encrypting organization laptop storage drives and memory lessens the impact of the threat of losing an organization laptop.

Implementation Plan

Immediate:	Encryption of all organization laptop drives and memory
Short Term:	Develop policies and procedures regarding when encryption for organization systems is required and what type of encryption should be used
Long Term:	Monitor and enforce adherence to organization encryption policies and procedures

Threat 2: Phishing Emails

The threat of phishing emails is a high-level risk to the Aspen Creek Power and Water organization. The impact of opening a phishing email could be tremendous due to techniques such as credential stealing and installing ransomware, which could significantly compromise business operations. Unfortunately, even without the recent incident of an employee opening a phishing email, successful phishing attacks are very common, which is why the likelihood score is the highest it could be at five.

Recommended Action

Aspen Creek Power and Water can mitigate most of the likelihood of a phishing attack threat through organization-wide employee training on how to spot phishing emails. This training would also make the organization compliant with NIST 800-53 AT-2(3) Social Engineering and Mining control through providing “literacy training on recognizing and reporting potential and actual instances of social engineering “(CSF Tools, 2024).

Implementation Plan

Immediate: Have organization employees complete external phishing training modules

Short Term: Develop social engineering policies and procedures along with a training program specifically tailored to Aspen Creek Power and Water employee needs

Long Term: Monitor and enforce employee completion of social engineering training

Threat 3: Remote Facility Break-in

The threat of a break-in to an Aspen Creek Power and Water remote facility is a medium-level risk to the organization. A break-in could result in the theft of organizational information systems such as laptops, unauthorized access or modifications to on-site information systems, and the theft of physical paper documents containing sensitive organizational information. These issues are why it was assigned a score of four for impact. The presence of security cameras, regardless of their operational state, does decrease the likelihood of an event occurring. However, due to some of the cameras being inoperable and the use of a keypad with a shared access code, the likelihood of a break-in is assigned a medium score of three.

Recommended Action

The main recommendation to mitigate the threat of a break-in to a remote facility is for Aspen Creek Power and Water to implement alarm systems at the electric substation along with both water treatment plants. Implementation of an alarm system would also put the organization in compliance with NIST 800-53 control PE-6(1) Intrusion Alarms and Surveillance Equipment. PE-6(1) requires organizations to “Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment” (CSF Tools, 2024).

Implementation Plan

Immediate:	Choose an intrusion alarm system vendor and engage in contract negotiations
Short Term:	Implement an intrusion alarm system in all facilities
Long Term:	Monitor the intrusion alarm service in all facilities

Conclusion

Due to the new Colorado security regulation, it is imperative that Aspen Creek Power and Water security program personnel review this security report and implement the recommendations to keep the organization aligned with the NIST 800-53 framework. While some areas of Aspen Creek Power and Water's security posture are adequate, the organization needs to implement employee training, more secure access controls, and encryption in all data states. Adherence to the NIST 800-53 cybersecurity framework not only secures business operations, but it also satisfies some regulatory requirements such as data privacy standards for the Federal Trade Commission Act Section 5 and cybersecurity standards the Federal Energy Regulatory Commission set in place in the NERC Critical Infrastructure Protection standards if the transmission of electricity is either coming in from or going out of state.

References

CSF Tools. (2024, December 6). *AC-2(9): Restrictions on Use of Shared and Group Accounts*. CSF Tools - The Cybersecurity Framework for Humans. https://csf.tools/reference/nist-sp-800-53/r5/ac/ac-2/ac-2-9/

CSF Tools. (2024, December 6). *AC-17(2): Protection of Confidentiality and Integrity Using Encryption*. CSF Tools - The Cybersecurity Framework for Humans. https://csf.tools/reference/nist-sp-800-53/r5/ac/ac-17/ac-17-2/

CSF Tools. (2024, December 6). *MA-6(1): Preventive Maintenance*. CSF Tools - The Cybersecurity Framework for Humans. https://csf.tools/reference/nist-sp-800-53/r5/ma/ma-6/ma-6-1/

CSF Tools. (2024, December 6). *PE-6(3): Video Surveillance*. CSF Tools - The Cybersecurity Framework for Humans. https://csf.tools/reference/nist-sp-800-53/r5/pe/pe-6/pe-6-3/

CSF Tools. (2024, December 6). *AT-2(3): Social Engineering and Mining*. CSF Tools - The Cybersecurity Framework for Humans. https://csf.tools/reference/nist-sp-800-53/r5/at/at-2/at-2-3/

CSF Tools. (2024, December 6). *PE-3(1): System Access*. CSF Tools - The Cybersecurity Framework for Humans. https://csf.tools/reference/nist-sp-800-53/r5/pe/pe-3/pe-3-1/

CSF Tools. (2024, December 6). *PE-6(1): Intrusion Alarms and Surveillance Equipment*. CSF Tools - The Cybersecurity Framework for Humans. https://csf.tools/reference/nist-sp-800-53/r5/pe/pe-6/pe-6-1/

CSF Tools. (2024, December 6). *SC-13: Cryptographic Protection*. CSF Tools - The Cybersecurity Framework for Humans. https://csf.tools/reference/nist-sp-800-53/r5/sc/sc-13/

Pfleeger, C. P., Pfleeger, S. L., & Coles-Kemp, L. (2024). *Security in Computing* (Sixth). Pearson.