CYBER SECURITY POLICY
For Managers of Drinking Water Systems

Excerpt from "Cyber Security Assessment and Recommended Approach," Final Report

STATE OF DELAWARE
DRINKING WATER SYSTEMS

February 2016

DPH Contract #15-361

Kash Srinivasan Group

Page intentionally blank

CYBER SECURITY POLICY DOCUMENT FOR MANAGERS

Version 1.0

This is a living document that helps you define how your organization will put in place, periodically review and update your policies and procedures related to cyber security. This policy defines how you intend to protect your organizations personnel and assets, the staff and outside contractors and vendors that are covered by the policy, and the processes you will use to assure compliance and meet your regulatory commitments.

This document was created in consultation with a SCADA system integrator with the express purpose of communicating cyber security needs and processes to decision makers and managers with non-informational technology backgrounds.

Disclaimer

This document is not intended as the sole guide for the implementation of cyber security for utility SCADA systems. Its purpose is to help facilitate the dialogue between utility managers and Information Technology and SCADA integration professionals so that utilities can arrive at the right suite of policies, procedures and technology appropriate to the local circumstance.

COMMENTS

Please provide critique and suggestions to help improve this document.

kash@ksgroupllc.com

TABLE OF CONTENTS

GOVERNING BODY

Designate the person or team with responsibility for establishing and overseeing compliance with the security policy. The team would typically consist of person in charge of the utility function, an information technology person and a risk manager to help define the cyber security rules applicable to the use of the system and the system configuration specific to cyber security risk mitigation.

CONFIGURATION MANAGEMENT

Limit functionality to reduce vulnerability

The configuration of the SCADA system and components should be based on the principle of "least functionality." Ensure that the SCADA team has conducted a criticality assessment of system components (servers, workstations, network components, application software). Critical components should, in general, have their functionality limited to the monitoring and control functions they are required to perform. Hardware and software elements should be carefully evaluated for need and only allowed to remain when the need is clearly established. These components should also be configured to provide for maximum security without impeding the functionality of the control network.

Disable all ports that are not needed for use by the system to prevent the unauthorized attachment and loading of programs through portable devices such as flash drives.

Control the software installation process

Installation, modification and upgrades of software programs must be restricted to, or supervised by, authorized users typically possessing "Administrator" privileges.   All applications to be installed must be pre-approved and the installation process must conducted by an authorized person whose identity is verified through a multi-factor authentication process (see Access Control)

ACCESS CONTROL

Identification And Authentication

Each user must be uniquely and positively identified before gaining access.

Prohibit sharing of passwords.

Password administration should require the use of strong passwords. This is an evolving area and the organization must periodically assess its definition of “strong” to stay current with best practice.

Assign a trusted individual (Administrator) as the keeper of passwords. Provide for the ability to reset passwords (either forgotten or expired).

Passwords should be changed frequently. Passwords must not be reused.

Include a challenge/response system to verify user authenticity.

Consider using a multi-factor authentication system – password and a physical token (such as a card) or a biometric system (e.g.; fingerprint reader) for access to sensitive control areas.

Principle Of Least Privilege

Limit users to only those functions they need to execute on the system to meet their assigned tasks. The user sign-on establishes the extent of access allowed.

System design should ensure that ports, protocols and operating system services are also limited in their functionality based on “least privilege.” If the system cannot achieve this goal by design, then other appropriate compensating controls must be provided. The local user should not have administrative privileges for the operating system of the workstation that accesses the SCADA control system.

Other

Disconnect the user after a certain idle period and require re-login. This prevents a workstation from remaining unattended. Disable Internet access from the SCADA workstation(s).

INTRUSION DETECTION AND INCIDENT REPONSE

An active incident response program must be in place in order to effectively monitor and respond to incidents, discover and handle security alerts and technical vulnerabilities, and collect and analyze security data. Monitoring could be some form of a physical system and/or a software program designed for this purpose.

PHYSICAL AND ENVIRONMENTAL SECURITY

Physical Access

Define areas that are openly accessible and areas that are restricted.

Make the area containing the SCADA system a restricted area. Limit access to this area(s) to authorized personnel.

Visitors to the SCADA area should be escorted and monitored.

Access to the area(s) is through an access device such as a key, a combination lock or key card system. On a periodic basis (established in your policy), change combinations and keys/cards.

Maintain logs of every entry to the restricted area(s).

Utility Power

Provide backup electric power to all SCADA components – Servers, Workstations, Programmable Logic Controllers (PLC), Remote Terminal Units (RTU), Network Switches – with appropriate Uninterruptible Power Supplies (UPS).

UPS units must receive the proper scheduled maintenance.

The utility should assess the probability and duration of power outages and select the backup-power systems accordingly.

ORGANIZATIONAL SECURITY AND INTEGRITY

Audit records are typically maintained by the SCADA system - tracking all actions taken, by whom and when. These records are available for review and must be reviewed on a periodic basis. Track all persons entering and leaving a secure area. The findings and anomalies encountered by the audit should be reported to the governing body.

The unauthorized re-setting of passwords and modification of system audit records can introduce vulnerabilities into the system and must be prevented. The system must be capable of restricting users from installing rogue software programs that can reset passwords and make other unauthorized changes.

MOBILE DEVICES

Mobile devices (laptops, tablets, smartphones, removable media (a.k.a. flash drives, thumb drives) and other such devices) represent a significant pathway for introducing unauthorized programs into the SCADA system.

Restrict connections to only those devices controlled by the organization. Enforce these restrictions.

Have a monitoring system in place that reports unauthorized connections. (See "Intrusion Detection and Incident Response" section).

Prevent the automatic execution of code on removable media without direction from an authorized user.

Travel by individuals with an organization-issued mobile device represents a significant risk; issue specially configured devices if such travel is a necessity. Establish and apply measures to mobile devices returning from risky locations to assure that unwanted code is not introduced into the SCADA system.

ADDITIONAL SYSTEM AND COMMUNICATIONS PROTECTIONS

Firewalls

The simplest SCADA arrangement is a closed system limited to Human-Machine Interface (HMI) devices and the PLC network. Unfortunately, it is frequently desirable to include the capability to access the system from outside this basic closed loop; users such as maintenance, and management staff may need information generated by the SCADA system for legitimate business purposes. System vendors also often need access to provide support to the system in the form of software upgrades. To facilitate these uses, a special purpose device [1] known as a firewall must be placed within the network to manage access from outside the basic SCADA loop. Firewalls should be properly configured to provide for maximum security without impeding the functionality of the control network.

[1] While usually a discrete piece of computer hardware, a firewall can also be implemented through software directly on a server.

Prevent unauthorized actions

A user has the ability to change set-points within automatic control loops and start and stop equipment remotely. These actions involve communication steps within the SCADA network. Discuss with your integrator/IT professional the methods they will use to manage this communication using IT methods such as "cryptography" and "key/certificate management." The outcome of these discussions should be captured in writing and used as Standard Operating Procedures as the SCADA system evolves.

Track remote access

If your system will need to support access from remote (outside the control room) locations (e.g.; telecommuting staff, off-hours response), ensure that acceptable methods of connecting to the SCADA system have been carefully considered before implementation. View-only access is the preferred method; additional protections must be in place if additional functionality is desirable. All remote access should be subject to monitoring and audit.

RESILIENCY

Resiliency is the ability to quickly recover operational control of a water system after a disabling event. Operations staff must possess the ability to take over manual control of the various components of a water system until normal operating modes are restored. A drawback of having a SCADA system in place is that the operations function has a "video-game" feel; hands-on operational skills could atrophy over time or be only minimally present in a new hire.

From a cyber security perspective, back-up devices and protocols must be in place to quickly restore SCADA system components and software.   The SCADA integrator must be actively engaged in the process of developing these response protocols.