EXHIBIT 2-A

Executive Summary (Public)
for
Cybersecurity Vulnerability Assessment and Security Posture Review

March 11, 2022

Prepared for:

Monterey Peninsula Water Management District

Prepared by:

Eugen Matei, CISSP, Cybersecurity Consultant

Contents

Executive Summary

Overview

Deveera Technology was contracted by the Monterey Peninsula Water Management District in September of 2021 to perform a Cybersecurity Vulnerability Assessment and Security Posture Review for the MPWMD. The approach to the engagement involved a physical site visit to review the organization's facilities and perform data collection regarding current operations, technical systems, and existing security practices operations. The second phase of the engagement involved remote security assessments and audits guided by the Center for Internet Security privacy controls. The result of the assessment met all requirements of the originating request-for-proposal (RFP) and included detailed reports of findings and actionable recommendations as final deliverables to the organization. The project was completed successfully.

This Project began in October 2021 and was completed in March 2022.
This Project included but was not limited to the following:

- Site visit and security walk-around of the MPWMD
- Meeting and interviews with relevant staff
- Custom approach to assessing additional MPWMD networks
- Depth-in-defense checklist for each MPWMD network
- Internal vulnerability network security scans
- External vulnerability network security scans
- Review of critical IT infrastructure and systems
- Review of current IT policies and procedures
- Review of special security concerns revealed during site visits

Overall Security Posture

The Monterey Peninsula Water Management District currently has an overall security posture rating of **LOW/MODERATE.** This rating is an indicator of how prepared the MPWMD is regarding current cybersecurity practices, policies, and operations that would protect the organization from cyber incidents.

The rating is derived from the compiled information attained through the recent security assessment. This security posture rating is the conclusion of the Security Consultant performing the Project and is also based on his experiences completing full quantitative CIS-mapped checklists of similar-sized local government organizations. Several recommendations are provided. Applying the recommendations can improve the overall security posture of the MPWMD.

From the perspective of MITRE's ATT&CK framework (Adversarial Tactics, Techniques & Common Knowledge), MPWMD Information System preventive and detective capabilities seem to be low/moderate, lacking detective capabilities across the board.

ATT&CK Activity	Preventive Capability	Detective Capability
Initial Access	Moderate	Low
Execution	Moderate	Low
Persistence	Moderate	Low
Privilege Escalation	Moderate	Low
Defense Evasion	Moderate	Low
Credential Access	Moderate	Low
Discovery	Moderate	Low
Lateral Movement	Moderate	Low
Collection	Moderate	Low
Command and Control	Low	Low
Exfiltration	Low	Low

MPWMD Information System security posture has been evaluated against the top 20 CIS Critical security controls and sub-controls mentioned in the table below, revealing an overall organization maturity level of 1.94 out of maximum 5.0.

Control	Family
1	Inventory and Control of Hardware Assets
2	Inventory and Control of Software Assets
3	Continuous Vulnerability Management
4	Controlled Use of Administrative Privileges
5	Secure Configuration for Hardware and Software
7	Email and Web Browser Protections
8	Malware Defenses

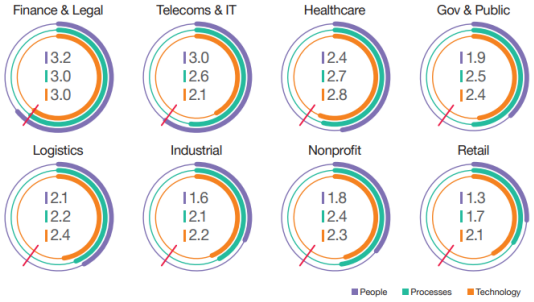
Control	Family
9	Limitation and Control of Network Ports
10	Data Recovery Capability
11	Secure Configurations for Network Devices
12	Boundary Defense
13	Data Protection
14	Controlled Access Based on the Need to Know
15	Wireless Access Control
16	Account Monitoring and Control
17	Implement a Security Awareness and Training Program
18	Application Software Security
19	Incident Response and Management
20	Penetration Tests and Red Team Exercises

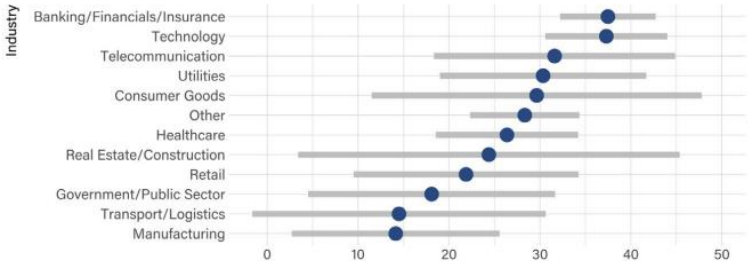
Maturity level:	Description:	Score:
Level One	Policies Complete	0.16
Level Two	Controls 1-5 Implemented	0.43
Level Three	All Controls Implemented	0.42
Level Four	All Controls Automated	0.36
Level Five	All Controls Reported	0.33

Maturity Rating*:	**1.71**

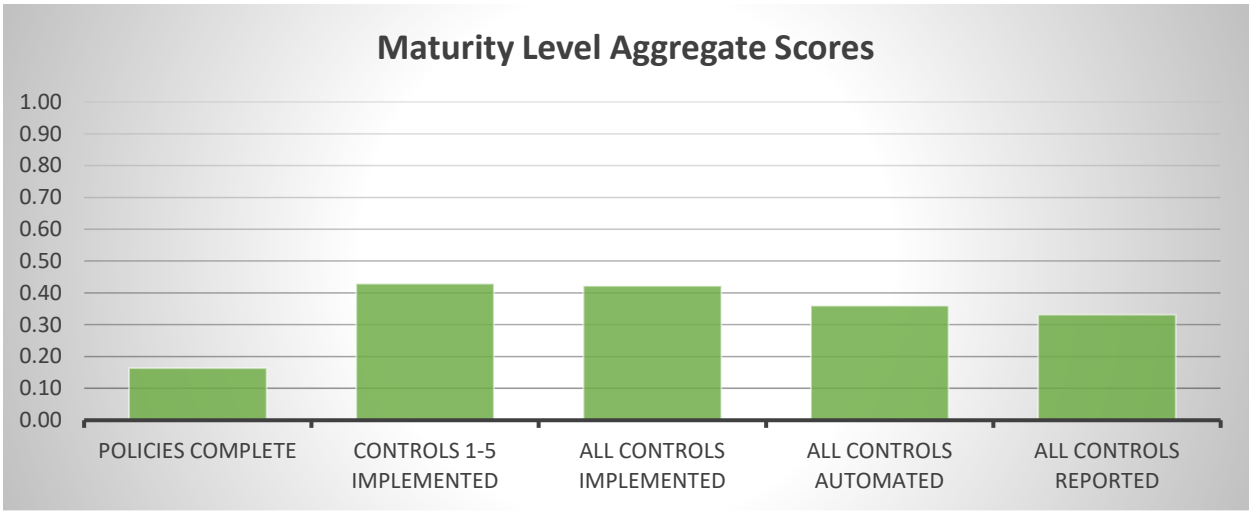
*Rating is on a 0-5 scale.

Comparison: Risk Maturity by industry





Ref: https://orangecyberdefense.com/global/white-papers/2019-security-maturity-report/
https://www.fairinstitute.org/2019-risk-management-maturity-survey-results-webianr



Top Cybersecurity Risk Items:

The security assessment led to the discovery of several areas of high-risk.

- Boundary Defense
- Maintenance, Monitoring, and Analysis of Audit Logs
- Inventory and Control of Hardware Assets
- Inventory and Control of Software Assets
- Data Protection

Risk Ratings Defined

Each security control is assigned a risk rating. Each risk rating considers impact, likelihood, and Information Security Maturity (ISM). Other mitigating controls and relevant risk factors are noted within each rating as described below.

Critical	There is limited evidence that controls and safeguards, to include key risk indicator controls, have been designed and implemented to protect organizational assets. Critical vulnerabilities with the presence of applicable threats exist within the environment assessed. A compromise of vulnerabilities is possible and likely based on the current state. A compromise could cause a serious and negative impact to the organization to include substantial financial loss, lack of compliance with regulatory or contractual requirements, and impact to the company brand and reputation. The organization would likely have an impaired ability to operate if the risks were realized.
High	There are a limited number of controls and safeguards that have been implemented to protect organizational assets. Vulnerabilities, to include critical, still exist and are in the presence of applicable threats. A compromise of vulnerabilities is possible and would cause a serious impact to the organization to include financial loss, lack of compliance with regulatory or contractual requirements, and impact to the company brand and reputation.
Moderate	The majority of the most critical controls and safeguards have been implemented to protect organizational assets. Vulnerabilities still exist and are in the presence of applicable threats. A compromise of these less critical vulnerabilities is possible and would likely be contained to a business unit or division within the organization. Exercised vulnerabilities could cause a negative impact including financial loss.
Low	All critical controls and safeguards have been implemented to protect organizational assets including additional compensating controls. There are no identified vulnerabilities in the presence of applicable threats at this time. Potential impact would be localized to the project level with minimal financial loss.

Summary of Recommendations

Administrative Controls

Administrative Controls form the framework for managing an effective security program and they are sometimes referred to as the "human" part of information security. Administrative Controls inform stakeholders on how organizational leadership expects day-to-day operations to be conducted and they provide guidance on what actions or activities workforce members are expected to perform. Common Administrative Controls include policies, security awareness training, guidelines, standards, and procedures.

Recommendations

- Develop a formal, written Cybersecurity Policy that addresses the specific operational needs
- Establish an Enterprise Risk Management strategy that associates cybersecurity investments with enterprise business plans

External Perimeter Technical Controls

External Perimeter Technical Controls are the controls that are technical in nature and used on the perimeter organization's technical domain (the gateways or firewalls). For the purposes of this assessment, switches, intrusion prevention systems, and wireless systems are included.

Recommendations

- Employ multifactor authentication
- Filtering tier for Internet facing web applications

Internal Systems Technical Controls

Internal Technical Controls are the controls that are technical in nature and used within the organization's technical domain (inside the gateways or firewalls). Internal technical controls include items such servers, Active Directory authentication, anti-virus software, and mobile device management (MDM).

Recommendations

- Operations Security: Implement centralized log/event collection system with reporting and correlation capabilities (SIEM)
- Implement asset inventory systems
- Network segregation/Access Control
- Server and Workstation Hardening
- Data Security

Conclusion

The Monterey Peninsula Water Management District has taken the best first step by implementing the comprehensive Information Security Assessment. The assessment serves as a guide and indicator for improvements regarding information security. The assessment can help catalyze the implementation of a formal Information Security Program to improve the security posture for the entire organization and all departments. However, actions taken by the organization after that initial report is issued, will define the quality and maturity of the way in which it handles security as time moves forward.

Threat actors (hackers) will continue to attack government systems, both targeted and untargeted, while frequency and intensity of attacks will continue to grow with time. The implementation of an information security program will put measures in place to assist the MPWMD moving forward. Systems change and new vulnerabilities will always develop. Implementing and maintaining information security is not a one-time event but an ongoing process. Keeping up with Information Technology is already a challenging task for all IT staff and technology service providers. Keeping up with Information Security is even more challenging and therefore, has evolved into its own profession.

Therefore, the single most important recommendation for the MPWMD is the establishment of an ongoing Information Security Program to address current risks and remediation's identified in the report and those to come in the future.

The two most important aspects of implementing a formal Information Security Program are to engage a security professional on a regular basis and to have that security professional report directly to the highest levels of administration.

The detailed Security Assessment Report has been provided to the management. However, due to the sensitivity of the contents, it will not be available publicly.