Proposed Orange County Sanitation District
Cyber Security Policy

Has OCSD properly prepared for the increase in cyber security threats faced by today's government agencies?

Summary Policy Statement

The Sanitation District must maintain adequate cyber security (information technology security) techniques that protect computer assets, networks, programs, data, and industrial control equipment from unauthorized access or attacks that are aimed for exploitation.

Background

Developing an effective, sustainable cyber security program is a pressing challenge for organizations of all sizes. The reasons behind the scope of the challenge are many. Cyber risk continues to grow at an exponential rate with routine attacks from nation states, criminal elements, hacktivists, and insider threats. The bottom line is cybercrime pays. The booming cybercrime economy is productizing malware and making cybercrime as easy as shopping at Amazon. With this easy access to cybercriminal tools and services, enterprises are experiencing rapid increases in the volume, scale, and sophistication of cyberattacks. Complex and dynamic information security disciplines are subject to continuous changes in the business, technology and threat environments. Many organizations will struggle to implement security programs that support continuous improvements in this challenging environment.

Current Situation

The Sanitation District has evolved over recent years from dedicating less than half of a position towards cyber security, to one position, to currently two full-time positions. The Sanitation District's cyber security portfolio consists of strategic policy management, defense in depth practices, periodic risk assessments, ongoing awareness communication and operational (e.g., security monitoring and incident response, threat and vulnerability management, user provisioning) processes. For example:

- Cyber Security Awareness and Training Program - The Sanitation District understands that our employees are our best line of defense in protecting and defending our enterprise from attack. We have built a comprehensive security awareness program by focusing on four critical functions: phishing attack simulations and reporting, quarterly education requirements, targeted training for IT developers and SCADA engineers, and pervasive communications utilizing internal communication tools.

- Vulnerability Management - IT staff subscribe to and monitor security advisories and threat bulletins from Microsoft, US-CERT, ICS-CERT, KnowBe4, Cisco, and other vendors to understand and manage new vulnerabilities. All internet accessible servers and applications are scanned weekly for vulnerabilities and remediated as necessary. Microsoft operating system and application patches

are deployed monthly while third party updates are deployed weekly. We use a vulnerability platform for continuous assessment of our security and compliance posture.

- Intrusion Detection and Response - We have implemented several security solutions to be able to detect, prevent and respond to malicious network activity. These include firewalls, intrusion prevent systems, web security gateway, and next-generation anti-malware. In addition, we also have user behavior analysis tools to identify insider threats and ransomware activity.

- Privileged Access Management Program - We use a privilege access management solution to remove and manage local administrative rights on workstations/servers to prevent lateral movement. The solution is also used to protect, control, and monitor privileged access across files and systems.

- Backup and Restore Capabilities – IT practices a 3-2-1 backup strategy:
  3 – Keep three copies of critical data
  2 – Have your data on two types of media
  1 – One copy must be offsite and offline

  Restores are performed on at least a weekly basis in response to customer incidents. Disaster Recovery Testing is performed monthly by selecting a major system and testing restore capabilities of that system to our secondary treatment facility, as well as our remote site. We sandbox the restores and provide access to our application subject matter experts to conduct application-specific testing. These tests are logged and kept for auditing and management purposes.

- Security Incident Response - An incident response plan is an organized approach to handle a cyberattack. We have developed an incident response plan, playbooks and procedures for various attacks as well as trained IT security staff. In addition, there are external contacts we can call for assistance including the FBI, Department of Homeland Security and organizations that specialize in incident response like Mandiant, Cylance, and Microsoft.

- Security Assessments - The purpose of a security assessment is to identify the current security posture of a system, network, or organization. The assessment provides recommendations to improve the security posture by mitigating identified risks. Our goal is to do one or two a year. The two most recently conducted assessments are the Office 365 Security Assessment from Microsoft in April 2019 and the Center for Internet Security Control Gap Assessment in July 2018.

Future Policy Statement

The main objective of our information security program is the establishment of a continuous, iterative regimen of planning, building, running and governing security capabilities that are derived from business requirements. Our security program cannot be a static entity. It must be adapted and continuously refined to keep pace with the ever-changing threat environment and changes in how the Sanitation District adopts digital business practices. Cybersecurity incidents are inevitable. Mistakes and/or a lack of preparation in the response can have serious repercussions. The ability of an organization to respond effectively to a security incident is a direct result of the time spent preparing for such an eventuality. If you fail to prepare, then you effectively prepare to fail. The Sanitation District will be prepared. This will be accomplished by the following proposed initiatives.

Initiatives to Support Progress Toward the Policy Goal

Initiative: Conduct various tabletop exercises to determine the organization's ability to respond to a targeted cyberattack and to improve the quality of the response, should an attack occur.

Initiative: Evaluate, enhance and monitor network security including activities to protect the usability, reliability, integrity and safety of the network by developing Security Operations Center capabilities that support continuous monitoring and is responsible for the continuous threat protection process.

Initiative: Conduct a comprehensive third-party cyber security operations assessment (Red Team). A thorough Red Team engagement will expose vulnerabilities and risks regarding:

- Technology — Networks, applications, routers, switches, appliances, etc.
- People — Staff, independent contractors, departments, business partners, etc.
- Physical — Offices, warehouses, substations, data centers, buildings, etc.